Business Security Report

Business Security Report 2017

Language: English

August 2017
Last revision date: 11th October 2017

www.av-comparatives.org

Contents

Introduction

AV-Comparatives' 2017 business software review looks at managed security products suitable for a company with a Microsoft Windows network. The review looks at some everyday tasks needed in networks. Full details of the points we have looked at for each program are given below.

Test System

Server: Windows Server 2016, Version 1607
Client: Windows 10, Version 1607

EDR features

Here we mention Endpoint Detection and Response features included in the product. EDR is defined by Gartner as "*the tools primarily focused on detecting and investigating suspicious activities (and traces of such) other problems on hosts/endpoints*."[1]

Management Console

Setup

A brief look at installing/configuring the management console so that the administrator can proceed with deploying endpoint protection software to clients.

Layout

Console design, with emphasis on finding major features.

Deployment methods for endpoint protection software

Deployment methods available, e.g. remote push, emailing a link to users, local installation on the client itself.

Monitoring the network

Status and alerts

How does the console show overall security status of the network, and warn of anything that the administrator should take action on, such as malware detections or outdated signatures?

Program version

Which version of the client software is currently installed on each device?

Managing the network

Scanning

How to run on-demand malware scans on protected devices.

Scheduling Scans

How to set up a regular scheduled scan.

Updates

How to run a manual update of malware definitions on managed clients.

[1] http://blogs.gartner.com/anton-chuvakin/2013/07/26/named-endpoint-threat-detection-response/

Removing devices from the console

If a device is lost, stolen or becomes unusable, how can its entry be deleted?

Controlling user access to the endpoint protection software

Options for making program features and configuration available to users.

Windows client protection software

A brief description of the user interface, i.e. whether it is a full GUI, limited GUI, or does not provide any interface for the user.

Tasks available to users

Whether the user can e.g. run updates and scans or change settings

Windows Security Center/Windows Defender

Whether the program registers as antivirus, antispyware and firewall (where appropriate) in Windows Security Center, and whether Windows Defender is disabled by the setup process.

Alerts

How does the program react if the EICAR test file is downloaded? How does it warn the user if real-time protection is disabled?

Windows server protection software

A brief guide to the user interface of the malware protection software for the server.

Console types

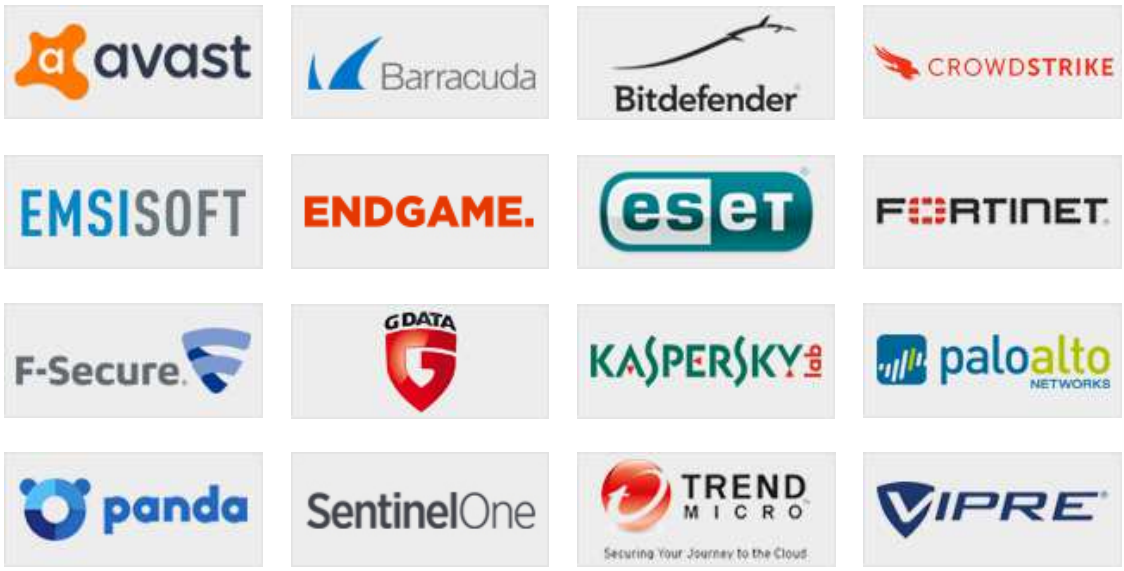
There are two main types of management console covered in this review.

Cloud-based consoles run on the manufacturer's servers. They can be accessed from any web browser on any Internet-connected device, by going to the URL provided by the manufacturer and logging in with the appropriate credentials. They have the advantages that no installation of the console is required, and that deployment of the client software is very straightforward for non-expert administrators. Additionally, a device can be monitored and managed easily wherever it is in the world, as long as it is connected to the Internet; this is obviously very useful for businesses with staff who frequently work outside of the office and are thus not connected to the company LAN.

Server-based consoles run on the company's own internal server on the LAN. Businesses are likely to need an IT professional to install the product. The user interface component of the program may be integrated into the program that runs on the server, available as a separate component that can be installed on the administrator's desktop or laptop PC, or accessible by web browser if a suitable HTTP server-function has been set up by the server component. Client-software deployment options may include those available for cloud-based consoles, with an additional option of remote push installation for devices connected to the company LAN. In this case, some configuration of client devices is usually necessary (such as enabling file sharing), after which the endpoint protection software can be sent out to multiple clients at once from the administration console. Server-based consoles may offer greater functionality than cloud-based ones, and some admins may prefer to have the system completely under their own control. Management of devices outside the LAN would require e.g. a VPN to be set up, however.

Products reviewed

The following manufacturers participated in this review:



The manufacturers either provided us with the newest versions of their respective products at time of testing, or confirmed that the latest version was available from their website. The products tested for the review are listed below:

1. Avast Business Antivirus Pro Plus 17.6
2. Barracuda NextGen Firewall 7.1
3. Bitdefender GravityZone Advanced Business Security 6.2
4. CrowdStrike Falcon Endpoint Protection 3.5
5. Emsisoft Enterprise Console 2017.7
6. Endgame Protection Platform 2.4
7. ESET Remote Administrator 6.5
8. FortiClient Enterprise Management Server 1.2
9. F-Secure Protection Service for Business 12.10
10. G DATA Business Security 14.0
11. Kaspersky Endpoint Security for Business Advanced 10.3
12. Palo Alto Networks Traps 4.0
13. Panda Adaptive Defense 360 7.70
14. SentinelOne Endpoint and Server Protection 1.8.5
15. Trend Micro Office Scan XG 12.0
16. VIPRE Endpoint Security Cloud 10.0

The reviews have been done using VMs, as a lot of companies are using virtualization, even on the clients. As those are all business products, vendors had the possibility to configure their products.

Management Summary

This report includes a wide variety of products. The question as to whether a product provides effective malware protection is answered by the certification test; a product can use any or all of its protection features to protect the test client, but the test result indicates only if the system was protected, not how. With regard to the management of each product, we note that some products require a new approach on the part of the administrator. For example, a firewall-based product that does not install any client software will require a different form of analysis from that used with a more conventional client-based endpoint protection product.

Avast for Business Premium Endpoint Protection is an endpoint security product with a cloud-based and on-premise console. We would say it is particularly suitable for small businesses without full-time IT staff. The well-designed console makes essential functions very easy to find, and the client software is familiar and equally easy to use.

Barracuda NextGen Firewall functions as an appliance that monitors and controls traffic to and from a company LAN. For larger companies with mostly office-based staff, it provides a whole new layer of protection, and can be used in conjunction with a client-based endpoint security product for maximum protection.

Bitdefender GravityZone Advanced Business Security is available in two different configurations. We have reviewed its cloud-based console (although an on-premises version in the form of a preconfigured virtual machine is available). Its clear design and customisation options make it very easy to use, and only minimal training would be required for non-expert administrators.

CrowdStrike Falcon Endpoint Protection requires some learning of new management techniques, but uses a well-designed cloud console that makes it easy to access features. It is probably better suited to larger businesses.

Emsisoft Enterprise Console is administered by an easy-to-install, server-based management console. Both this and the endpoint protection software are clearly designed and easy to navigate, making everyday administration an easy task for all administrators.

Endgame Protection Platform is available as an on-premises or cloud-based console. Whilst it requires learning some new management techniques, its console is well designed and easy to navigate, making it straightforward to discover the product's functionality. We feel it is better suited to larger companies with their own IT departments.

ESET Remote Administrator is administered using a console that can be installed on a local server, or run as a virtual machine locally or on Microsoft Azure. Clear design of both console and client software, along with excellent help features, make everyday management very straightforward.

Fortinet Enterprise Management Console is a very well-designed, server-based modern administration tool for managing endpoint protection software. Good documentation makes deployment easy, and non-expert administrators would be able to perform day-to-day administration tasks with minimal training.

F-Secure Protection Service for Business uses a cloud-based console for the management of endpoint security software. The very clean, simple and modern design of both console and client software make essential features very easy to find, and consequently we feel the product is especially suitable for small businesses without full-time IT staff.

G Data Business Security provides an endpoint security product with a server-based console. Experienced administrators will feel very much at home with installation and deployment, and non-expert administrators will have no difficulty with everyday management tasks.

Kaspersky Endpoint Security for Business Advanced has a server-based console. It uses Microsoft's MMC console as a foundation, making it very familiar and easy to navigate for Windows administrators. It is a fully scalable solution, facilitating comprehensive management and easy separation of administrator responsibilities, all from a single, unified console.

Palo Alto Networks Traps is typically supplied as an on-premises server solution, and is probably best suited to larger companies with their own IT staff. Although some new management techniques are required, the console design makes it easy to discover and use the product's features.

Panda Adaptive Defense 360 is managed by a well-designed, clearly laid-out cloud-based console, which would be very straightforward for less-experienced administrators to use. This makes it particularly suitable for small businesses, while its EDR features will make it appealing to corporations too.

SentinelOne Endpoint and Server Protection provides a choice of server-based or cloud-based consoles. Whilst the nature of the product means that the admin will have to learn some new management techniques, the console is very well designed and easily navigated. Comprehensive information on threats and activities is provided.

Trend Micro OfficeScan uses a server-based console to manage endpoint security software. Whilst it is capable of managing larger networks, we found it very simple and unproblematic to install and use, meaning that it would be suitable for smaller companies too.

VIPRE Endpoint Security Cloud uses a cloud-based console to manage endpoint security software for Windows clients and servers. We found it extremely simple to use for all deployment and management tasks, and it thus stands out as an ideal solution for smaller businesses without permanent IT staff.

AV-Comparatives Approved Business Product Award 2017

As part of the certification of business security products, we ran a Real-World Protection Test using our Real-World Testing Framework.

To get the Approved Business Product Award, the reviewed business products had to achieve at least a 90% protection rate, with no false positives on business-related software.

This year, we are once again pleased to report a very high overall standard, and that all the products reviewed receive our Approved Business Product award.

Avast Business Antivirus Pro Plus

Overview

Product version reviewed

Avast Business console 3.2.34
Avast Business Security for Windows clients and servers 17.6.2525

Windows operating systems supported

Clients: Windows XP, Vista, 7, 8, 8.1, 10
Servers: Windows Server 2008 R2, 2012 R2, 2016
Avast Business Antivirus Pro Plus uses either a server-based or a cloud-based console to manage Windows and Mac OS clients, and Windows Servers. We have reviewed the cloud-based console here.

EDR features

Avast Business Antivirus Pro Plus does not currently include EDR features.

Product information on vendor's website

https://www.avast.com/business-antivirus-pro-plus

Online support

https://www.avast.com/business-support

Summary

We feel that Avast Business Antivirus Pro Plus is exceptionally well suited to small business environments, especially those without full-time IT staff. We found the console very easy to navigate, with all the important functions very straightforward to find and use. Installing and using the client software will be very familiar to anyone used to consumer antivirus programs. We were also impressed at how fast the console updated to show changes made on the client, and vice versa.

Tips for administrators

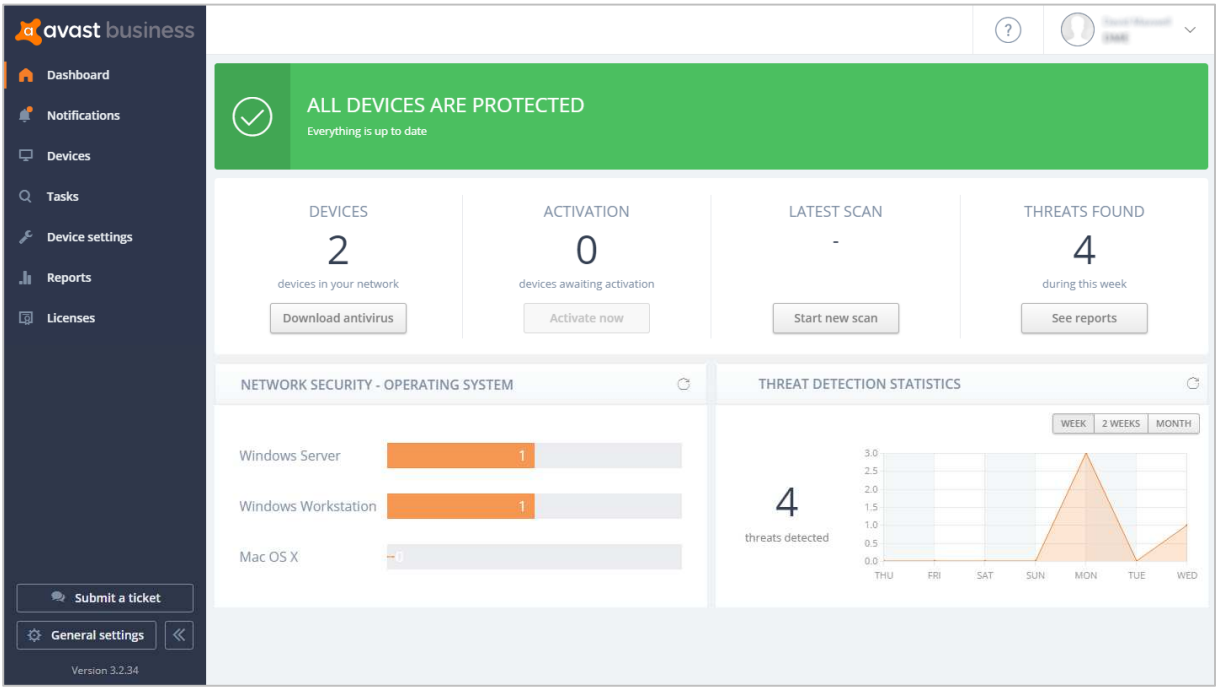
We suggest that administrators make use of the password-protection feature, to prevent users from changing program settings.

Management Console

Installation and configuration

The console is cloud-based, so no installation is required.

Layout



The console can be navigated very easily using the menu panel on the left-hand side.

Dashboard provides an overall status display, shown above.

Notifications shows malware alerts and other notifications.

Devices lists devices on the network and allows tasks to be carried out (see screenshot further down).

Tasks shows tasks (such as scans and updates) already created and lets the admin create new ones.

Device Settings displays settings templates (policies) and allows these to be edited (see screenshot further below).

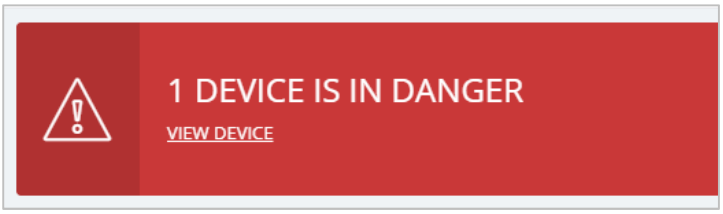
Deployment methods for endpoint protection software

- Download from console and install directly on local computer
- Email installation link to users

Monitoring the network

Status and alerts

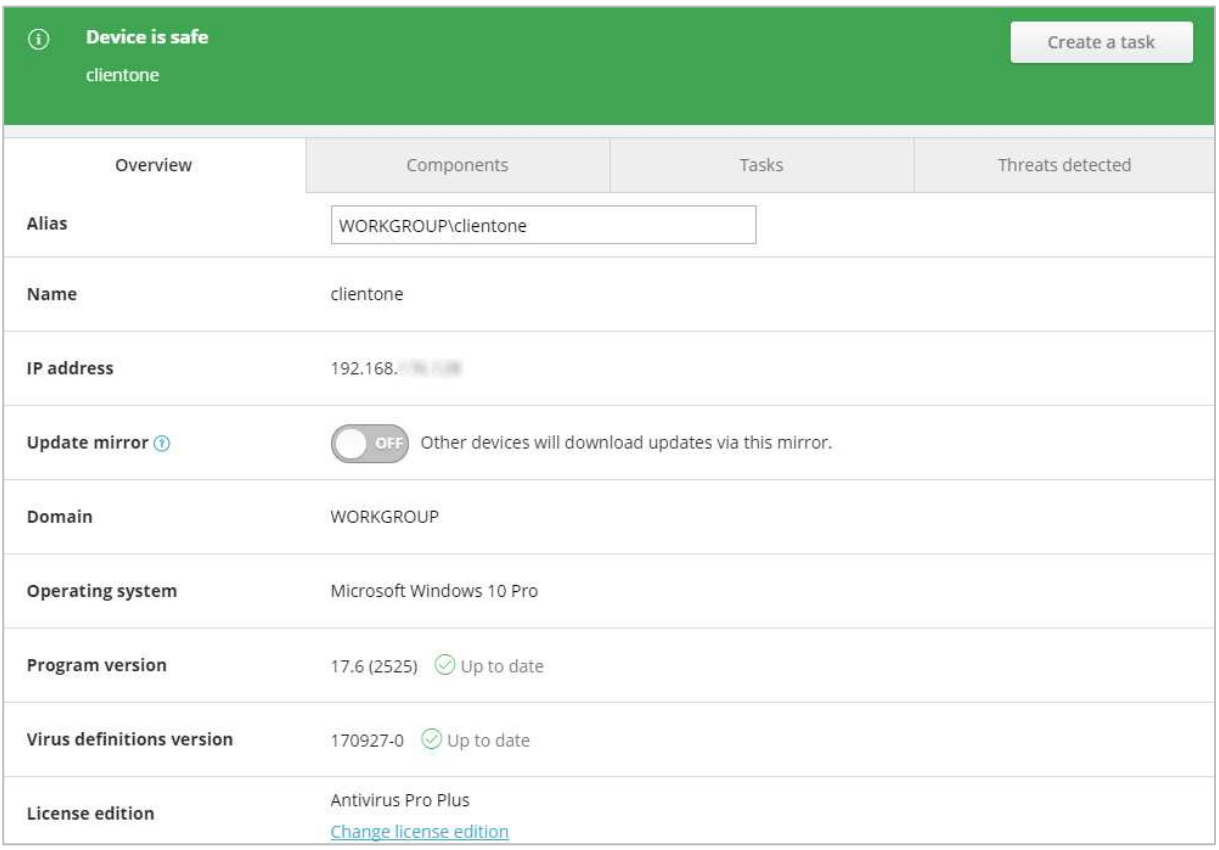
The *Dashboard* page has a simple overall status display at the top, which is green if all is well, but turns red to show alerts:



In our test, we found that the status display responded very quickly – within a few seconds – if e.g. protection was switched on or off.

Program version

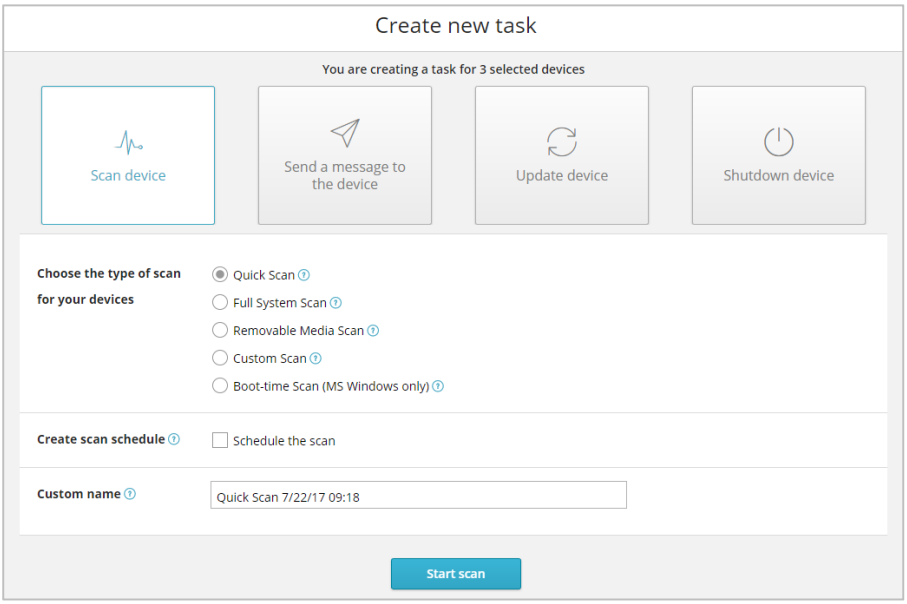
Clicking on an individual PC on the *Devices* page provides detailed information for that device, including the endpoint protection program version:



Managing the network

Scanning, scheduling scans, updates and removing devices from the console

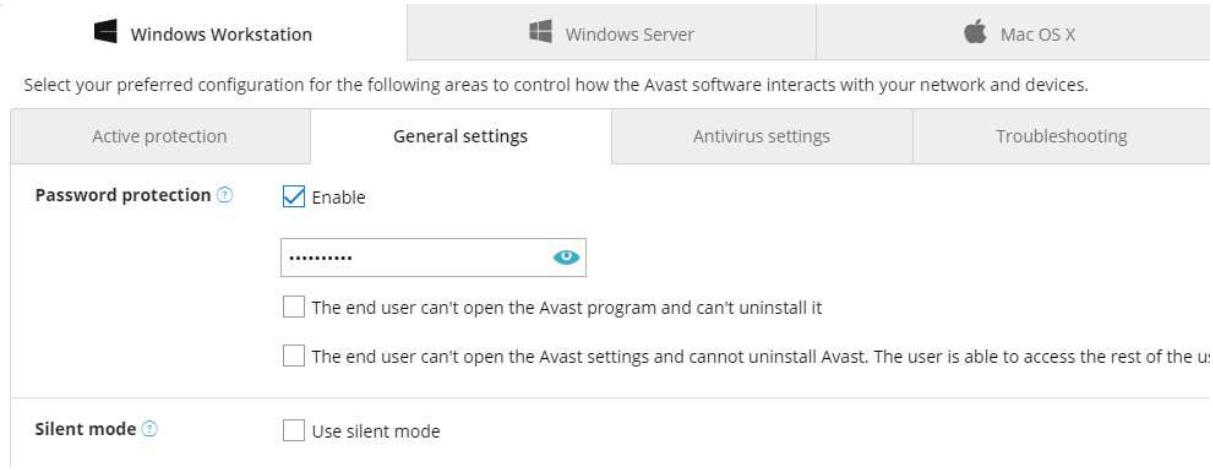
All these actions can be performed by selecting computers on the *Devices* page, then clicking the *Actions* menu. Scans can be run by clicking *Create a task* in this menu. The following page opens:



The page can also be used to send a message for the user, and restart/shut down the device. All the tasks can be scheduled.

Controlling user access to the endpoint protection software

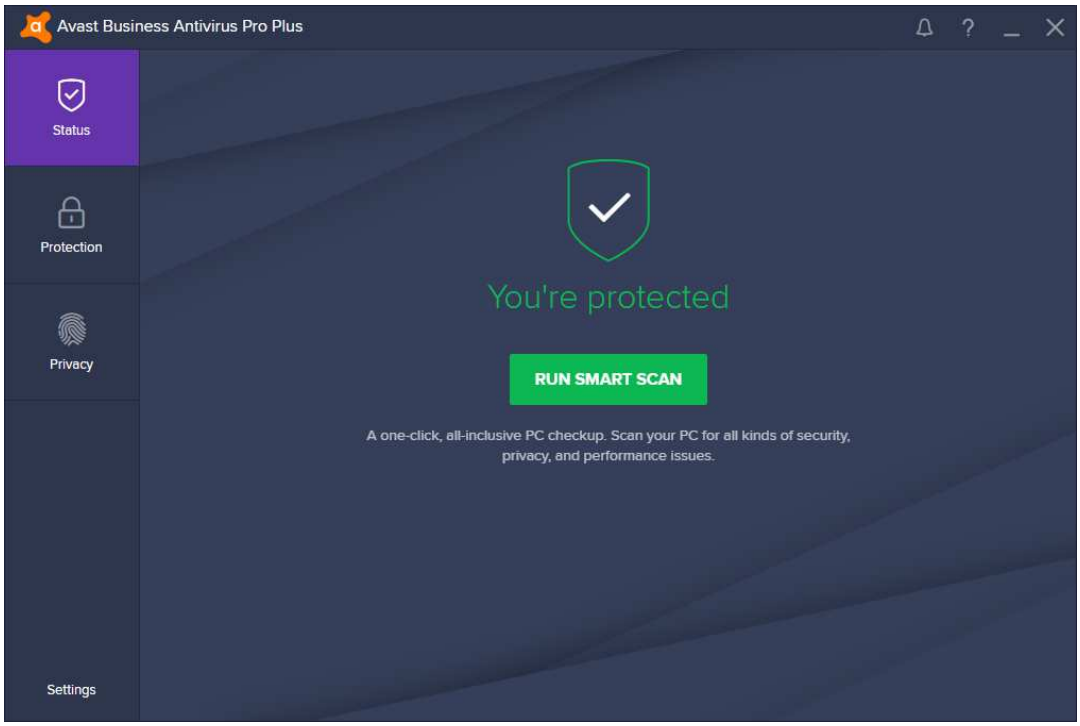
By default, all users have full control over the client software. However, settings can be password protected by clicking *Settings*, then the relevant settings template (policy); this opens the settings page shown below:



We note that the administrator can create different settings for Windows workstations, Windows servers, and Mac OS workstations (in addition to different device groups).

Windows client endpoint protection software

There is a full GUI, similar to a consumer antivirus program:



Tasks available to users

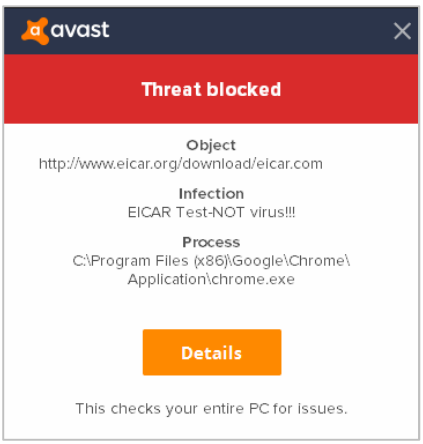
If password protection has not been set up, users have access to all the functionality, including settings, updates and quarantine. If the admin does enable password protection, he/she can choose between letting users access the GUI and run scans, and completely blocking user access to the GUI.

Windows Security Center/Windows Defender

Avast Business Antivirus registers in Windows Security Center as the antivirus and firewall programs. Windows Firewall and Windows Defender are disabled.

Alerts

If the EICAR test file is downloaded, the alert below is shown:



No user action is required. The alert disappears after about 10 seconds.

If real-time protection is disabled, the main program window shows an alert:

The user can reactivate the protection by clicking *Turn on*.

Windows Server endpoint protection software

This can be regarded as identical to the client software, although it is automatically configured during installation so that components not relevant to a server, such as the Avast firewall, are not installed.

Barracuda NextGen Firewall

Overview

Product version reviewed

Barracuda NextGen Firewall F-Series 7.1.0 Build 371
on VMware ESXi managed by NG Admin Application 7.1.0 Build 491

Supported virtualization platforms and Windows operating systems

Firewall: The Barracuda NextGen Firewall can be supplied as a preconfigured virtual machine for VMware ESXi version 3.5 or higher, Citrix XenServer 6.2 or higher, open-source Linux XenServer 4.x or higher, KVM 5.4.2 or higher, and Microsoft Hyper-V. Hardware appliances and cloud-based appliances for Amazon AWS, Microsoft Azure, and Google Cloud Platform are also available.

Administration console: This runs as a standalone executable on Windows 7, 8/8.1, 10

About the product

As its name suggests, the product includes a next-generation firewall with application and user awareness. As the product is network-based rather than client-based, there is no client software to install on workstations or Windows servers. Consequently, the functionality described in this review differs from that of traditional antivirus products. Product features include Avira's signature-based antivirus engine, and Barracuda's own Advanced Threat Protection (ATP) feature. ATP is a cloud-based sandboxing service specialized in real-time malware-analysis by running suspicious files on various operating systems. In the absence of any client software, a third-party endpoint antimalware product can and should be deployed on clients as additional protection layer; this would be essential for any devices that are used outside of the company LAN. For VPN / SSL-VPN remote access Barracuda Networks provides free full VPN client software for Windows, macOS, and Linux as well as iOS and Android.

EDR features

With regard to EDR features, Barracuda state the following: "*As part of the optional Advanced Threat Protection capability, the Barracuda NextGen Firewalls detect botnet command & control traffic, block the traffic to prevent data exfiltration, and can automatically move the affected clients into a quarantine network. Barracuda NextGen Firewall is a network-based security and traffic-optimization device and offers no other EDR features by itself. However, Barracuda NextGen Firewall provides a REST-based API interface for integrating the SIEM or EDR tool of choice to block traffic to/from an infected device or deviate traffic from a detected device. Barracuda NextGen Firewalls F-Series are integrated to the Splunk SIEM system*".

Product information on vendor's website

https://www.barracuda.com/products/ngfirewall

Online support

https://www.barracuda.com/support

Summary

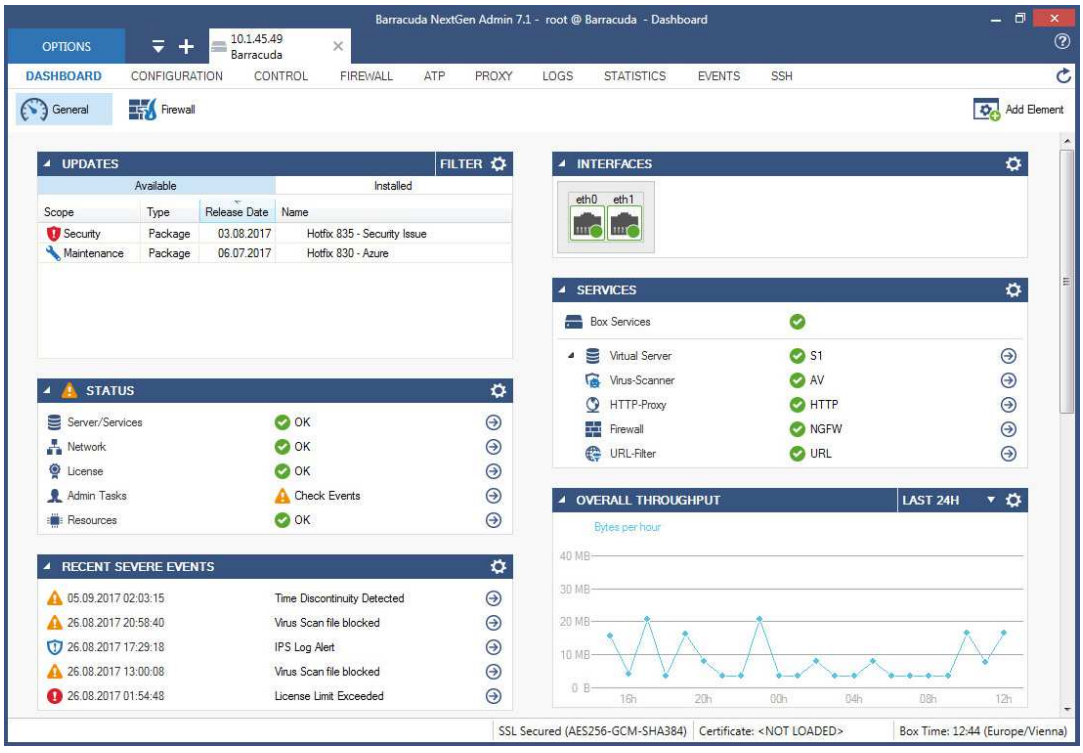
Barracuda NextGen Firewall provides protection for all the devices within a company LAN. By its nature, it's less suited to smaller companies with limited infrastructure or to companies with a high percentage of staff members working outside the company office. However, for larger companies, it provides an entire layer of additional protection that supplements rather than replaces traditional endpoint protection software.

Management Console

Installation and configuration

The functionality of the firewall is provided by the preconfigured virtual machine, which needs to be incorporated into the company virtualisation platform. The network then needs to be configured so that the firewall functions as a gateway for the LAN. A Barracuda technician assisted us with the configuration of the firewall, as is their standard practice for customers. The administration software is a standalone executable and does not need to be installed. After starting the software, administrators only need to enter the IP address of the firewall and their login credentials to access the management console.

Layout



The console opens on the *General* tab of the *Dashboard* page, providing mostly status information, as well as a list of recently detected threats. Administrators may also choose to hide some sections from the *Dashboard* page, allowing them to concentrate on the most important items for them. The menu at the top of the console window allows navigation to the other main pages: *Configuration*, *Control*, *Firewall*, *ATP*, *Proxy*, *Logs*, *Statistics*, *Events*, and *SSH*. The content of each page is further divided into multiple tabs.

Deployment methods for endpoint protection software

In keeping with the nature of the product, there is no endpoint software to be deploy.

Monitoring the network

Status and alerts

Apart from the status overview and a short list of recent threats on the *General* tab, the main page also provides the *Firewall Dashboard* that list threats encountered by the system. More details about detected threats can be retrieved from the *Firewall* main page of the console. The *ATP* (Advanced Threat Protection) tab provides a list of detected threats. Administrators can download a report for each threat, including detailed static and dynamic analysis.

Program version

The major program version of the administration software is displayed in the title bar of the console window. More detailed information about the software version running can be obtained from the *Options* menu.

Managing the network

Scanning, scheduling scans, updates and removing devices from the console

The firewall automatically scans incoming and outgoing Web, FTP and Mail traffic for threats. Built-in deep SSL-Inspection extends this to encrypted communications (HTTPS/SMTPS) via a sanctioned man–in-the-middle approach. Additionally, administrators can manually upload malicious files for analysis in the sandbox.

Bitdefender GravityZone Advanced Business Security

Overview

Product version reviewed

Bitdefender Endpoint Security 6.2.22.923

Windows operating systems supported

Clients: Windows XP, Vista, 7, 8/8.1, 10
Servers: Windows Server 2003/R2, 2008/R2, 2012/R2; Windows Small Business Server 2003, 2008, 2011. In our test, Bitdefender Endpoint Security worked flawlessly with Windows Server 2016.

About the product

Bitdefender GravityZone uses a cloud-based console to manage security software for Windows, Mac and Linux operating systems. Bitdefender GravityZone console comes also in an on-premise version, but for this test the cloud-based version was used.

EDR features

With regard to EDR features, Bitdefender state the following: "*In the last quarter of 2017, Bitdefender will introduce "Bitdefender xDR" that amalgamates threat prevention, threat detection and threat response capabilities into a single solution. "Bitdefender xDR" will prevent known and unknown attacks, detect suspicious activities on the device, investigate the activities to understand impact and confirm presence of indicators of compromise. Attacks are validated by Bitdefender Sandbox Analyzer and Bitdefender Global Protective Network. Incident response actions include: deleting IOC's, quarantining affected systems and tuning protection policies to automatically prevent future attacks*".

Product information on vendor's website

https://www.bitdefender.com/business/elite-security.html

Online support

https://www.bitdefender.com/support/business/

Summary

Bitdefender GravityZone's console requires no installation or configuration, and we found its design to be very clean, simple and easy to navigate. We liked the fact that the *Dashboard* page can easily be customised to show different alerts or status items, and the installation options dialog that is (optionally) displayed after logging in makes deploying client software very simple. The client software is also very clearly designed, and allows users to perform essential everyday tasks.

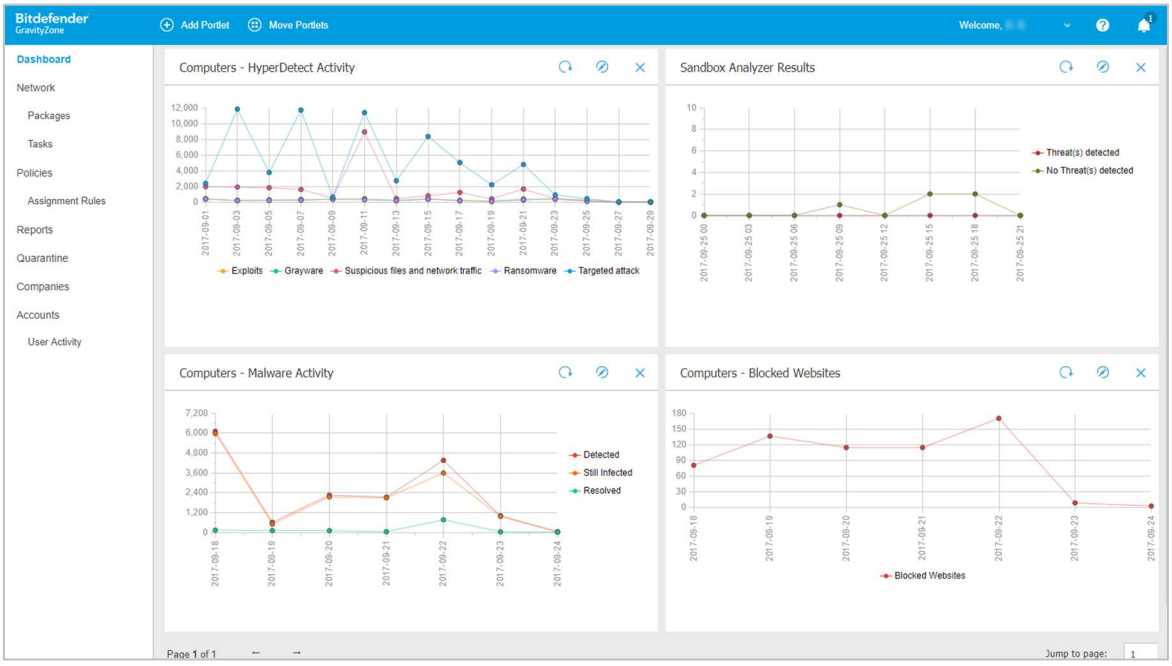
Whilst having the functionality needed to cope with larger networks, we feel the simplicity and ease of use make Bitdefender GravityZone particularly suitable for companies without full-time IT staff.

Management Console

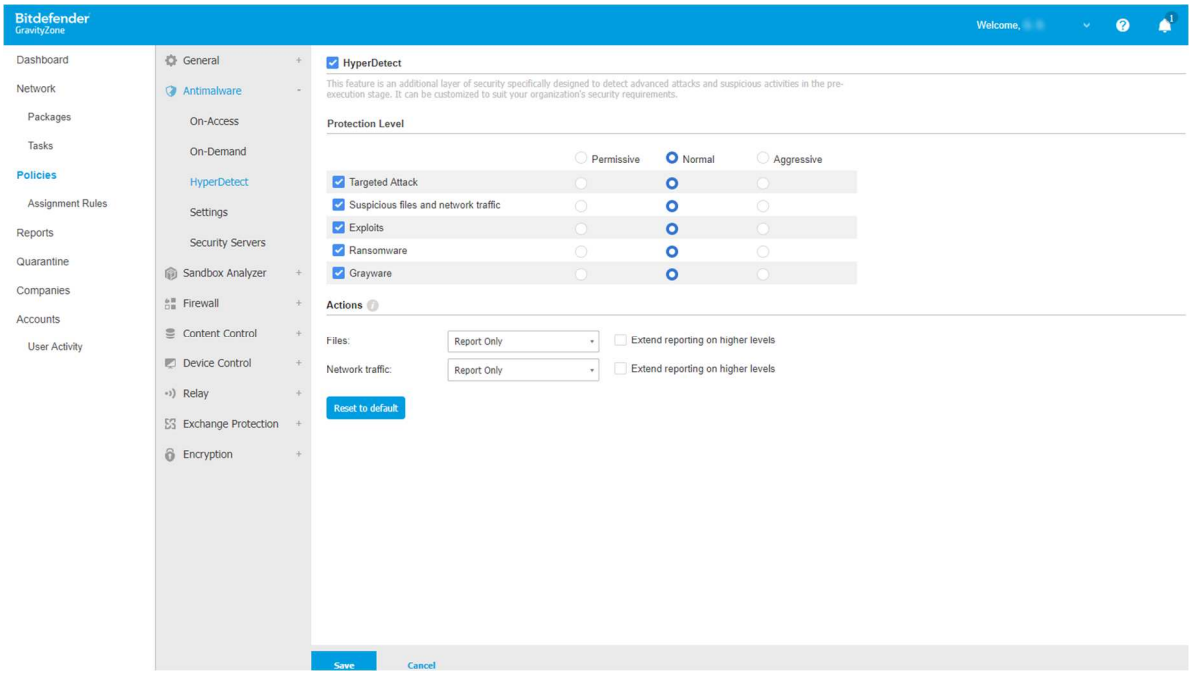
Installation and configuration

The console is cloud-based, so no setup is necessary.

Layout



The console has a very simple and familiar design, with a menu column on the left-hand side allowing the admin to switch between *Dashboard, Network, Policies, Reports, Quarantine* and *Accounts*.



Deployment methods for endpoint protection software

- Download and install locally from client
- Email installation link to users
- Remote push installation from first preinstalled client

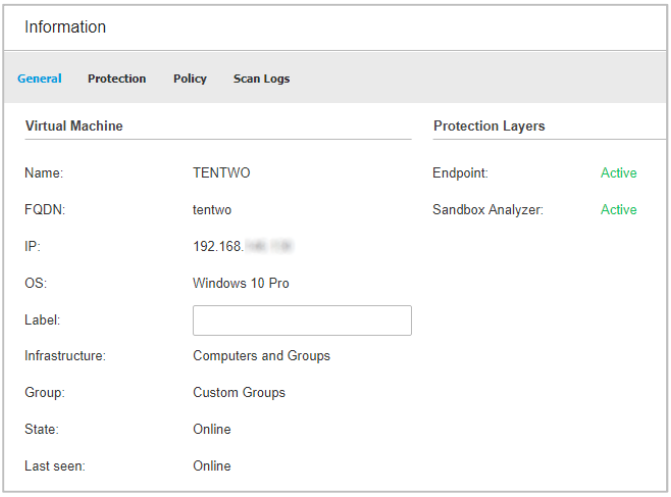
Monitoring the network

Status and alerts

These are shown on the *Dashboard* (home) page of the console, and consist of *Malware Activity, Malware Status, Top 10 Detected Malware,* and *Endpoint Protection Status*.

Program version

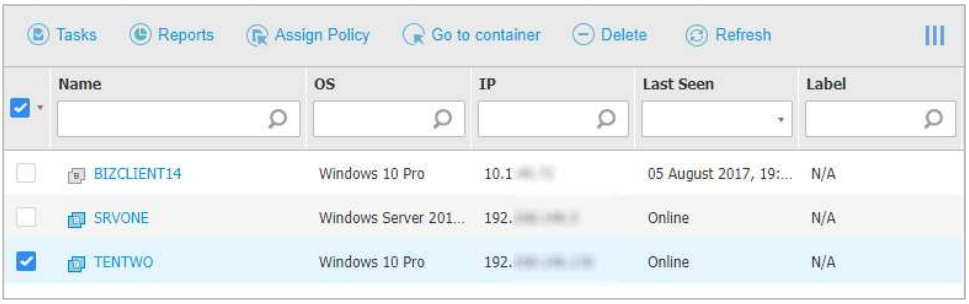
This is displayed on each client's *Information* page, found by clicking its entry on the *Network* page:



Managing the network

Scanning, scheduling scans, updates and removing devices from the console

On the *Network* page, the admin can select computers, assign tasks such as updates and scans, or policies:

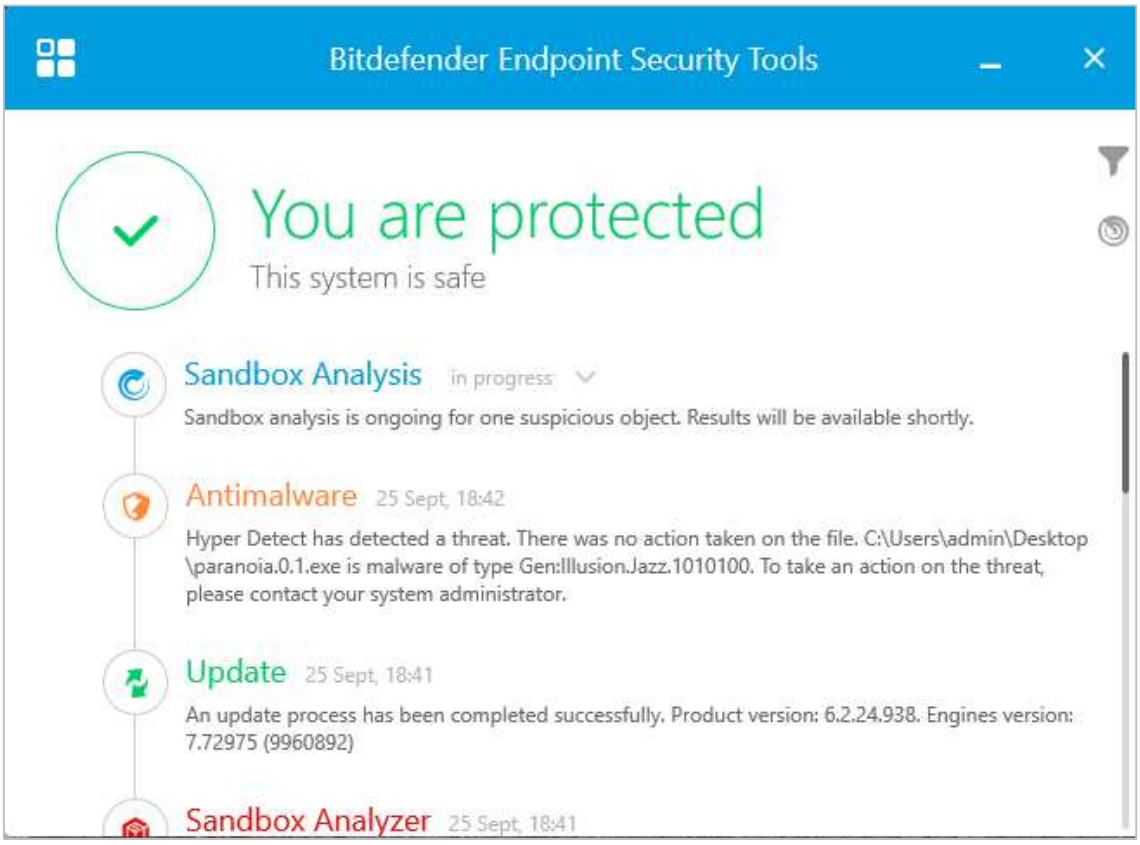


Controlling user access to the endpoint protection software

By default, all users are prevented from disabling protection components.

Windows client endpoint protection software

The client software has a GUI with a prominent status display, and controls for functions and settings:



Tasks available to users

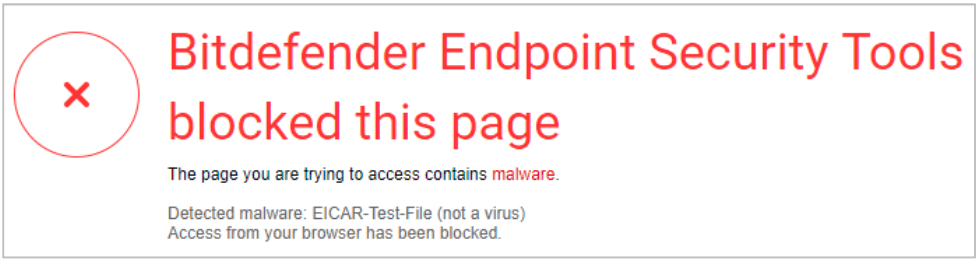
Users can run quick, full or custom scans, and check for updates.

Windows Security Center/Windows Defender

Bitdefender Endpoint Security Tools registers as the antivirus and firewall programs in Windows Security Center. Windows Defender and Windows Firewall are disabled.

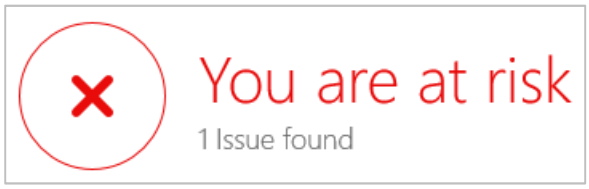
Alerts

If the EICAR test file is downloaded, the file is blocked and the alert below is shown in the browser window:



No user action is required.

If real-time protection is disabled, a warning is shown in the status area of the main program window:



By default, components can only be activated or deactivated from the console.

Windows Server endpoint protection software

This can be regarded as identical to the client software, although some components (firewall, content control) are not installed.

CrowdStrike Falcon Endpoint Protection

Overview

Product version reviewed

CrowdStrike Falcon Sensor 3.5.5606

Windows operating systems supported

Clients: Windows 7, 8/8.1, 10, all 32 and 64-bit)
Servers: Windows Server 2008 R2, 2012/R2, 2016
CrowdStrike Falcon also supports Mac and Linux operating systems.

About the product

CrowdStrike Falcon uses a cloud-based console to manage protection for all clients. Please note that the prevention features need to be turned on for the product to automatically block threats.

EDR features

With regard to EDR features, CrowdStrike states the following: *"CrowdStrike simplifies endpoint detection and response (EDR) for business users. The product records all endpoint activity and does three things with the data to enhance protection. First, it uses the data to paint a complete picture of activities surrounding an attempt to run malware, enabling security teams to work smarter and faster by understanding the attack. Second it uses behavioral analytics to automatically identify and block file-less and malware-free attacks. Third it stores the data in the CrowdStrike ThreatGraph(TM) so that businesses can quickly hunt for threats or investigate incidents; the Falcon Overwatch team also works 24x7 to hunt for threat activity in this data set, acting as a partner to provide proactive protection for all organizations."*

Product information on vendor's website

https://www.CrowdStrike.com/products/

Online support

https://supportportal.CrowdStrike.com

Summary

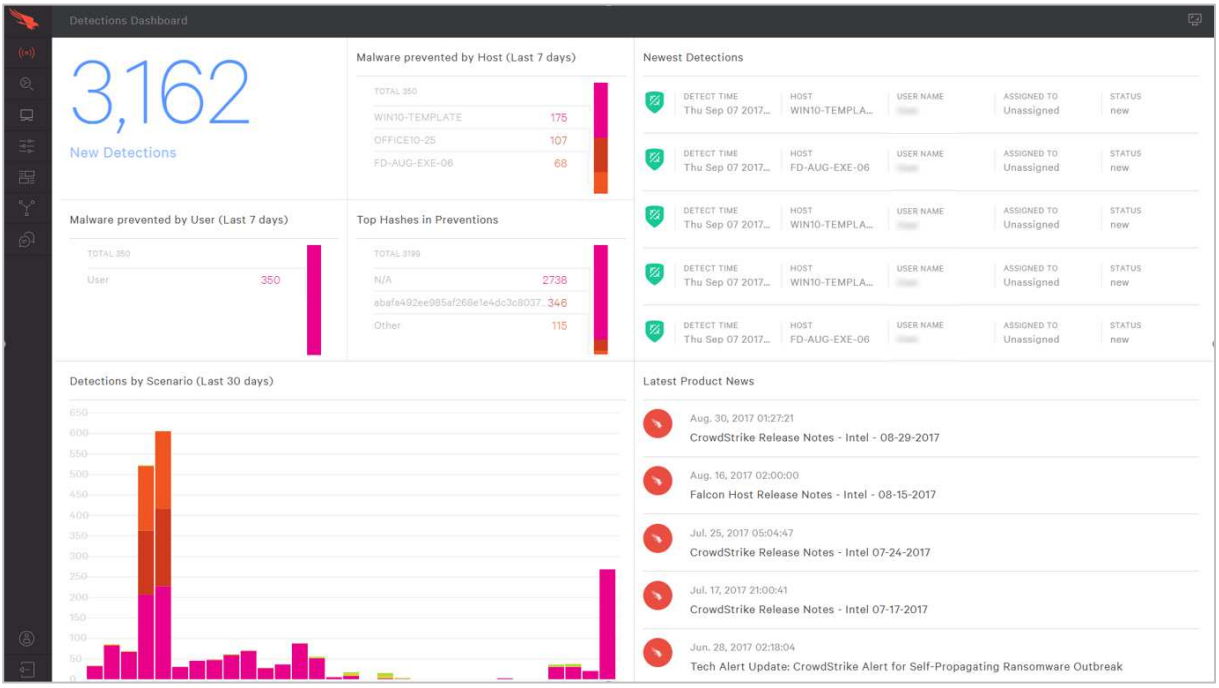
The management console is well designed and easy to navigate, allowing administrators to explore the functionality with ease. A wealth of detailed information on threats etc. is provided. The product is probably better suited to businesses that have their own IT department.

Management Console

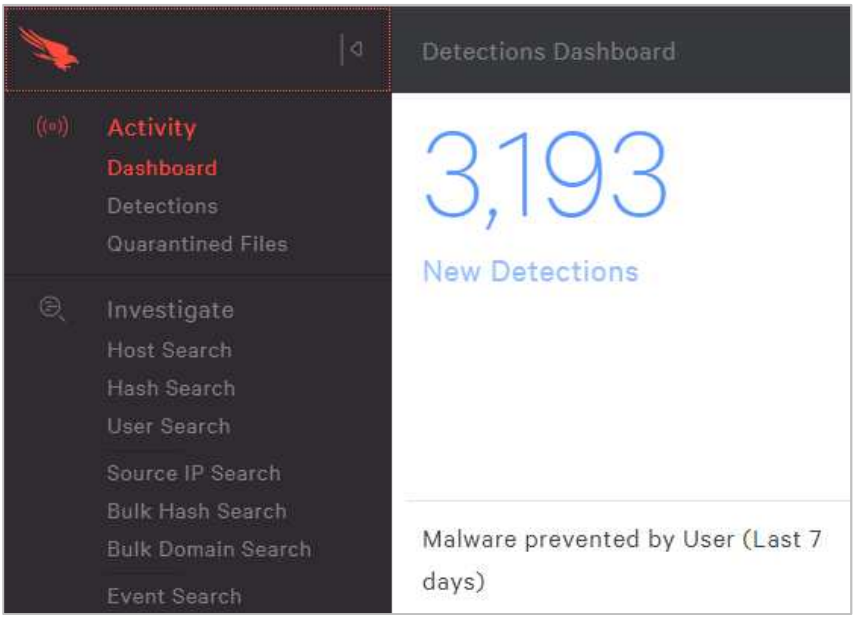
Installation and configuration

The console is cloud-based and so no installation is necessary.

Layout and functionality



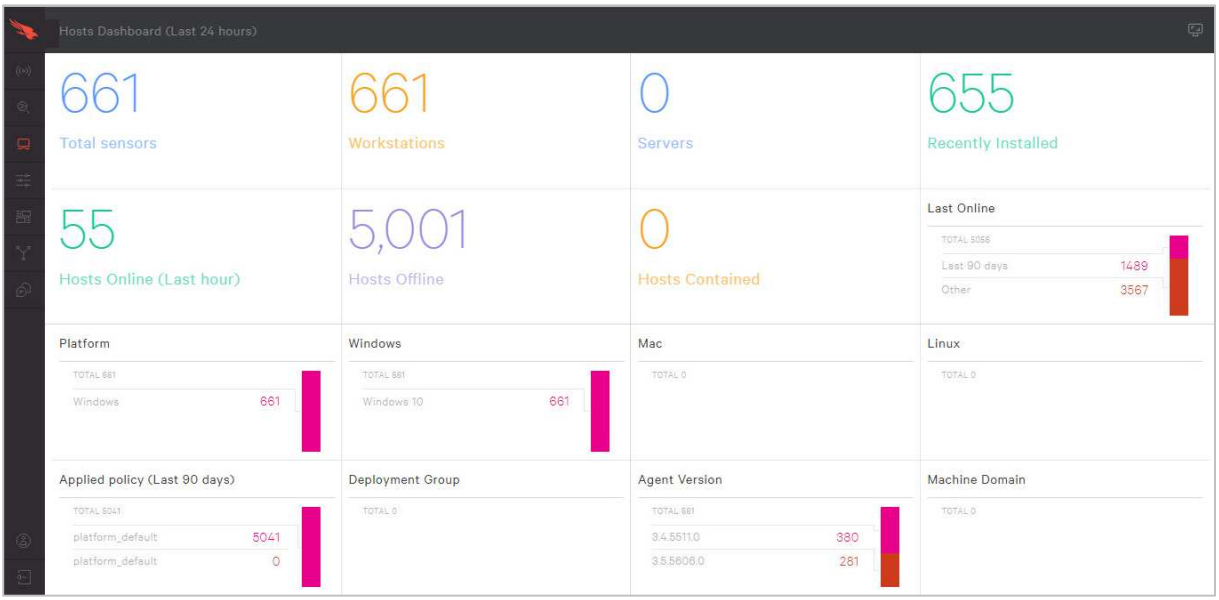
The console is navigated by means of a left-hand menu bar, with the main items *Activity, Investigate, Hosts, Configuration, Dashboards, Intelligence* and *Support*. This can be expanded by clicking the red Falcon graphic in the top left-hand corner, thus displaying the names and sub-pages for each of the items:



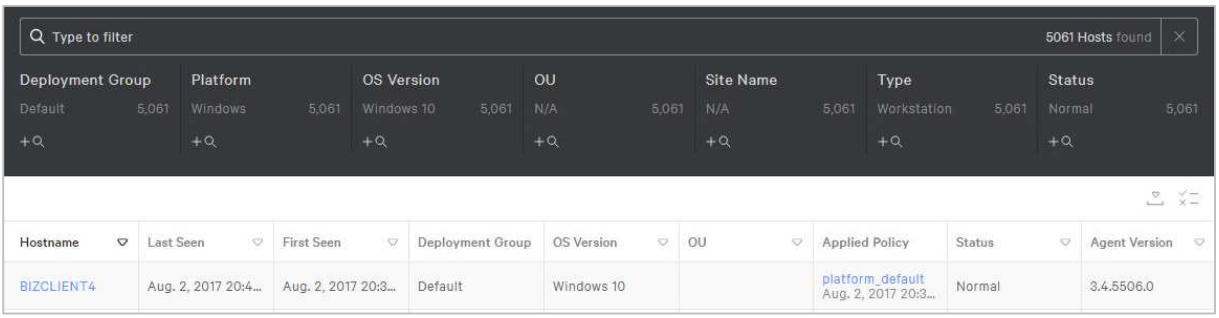
The *Activity Dashboard* (home) page of the console shows a variety of detection statistics, including *New Detections, Malware prevented by Host, Newest Detections* and *Detections by Scenario*.

The *Investigations* page allows the admin to search for any item collected by the Falcon agent, including hosts, hashes, users and source IP.

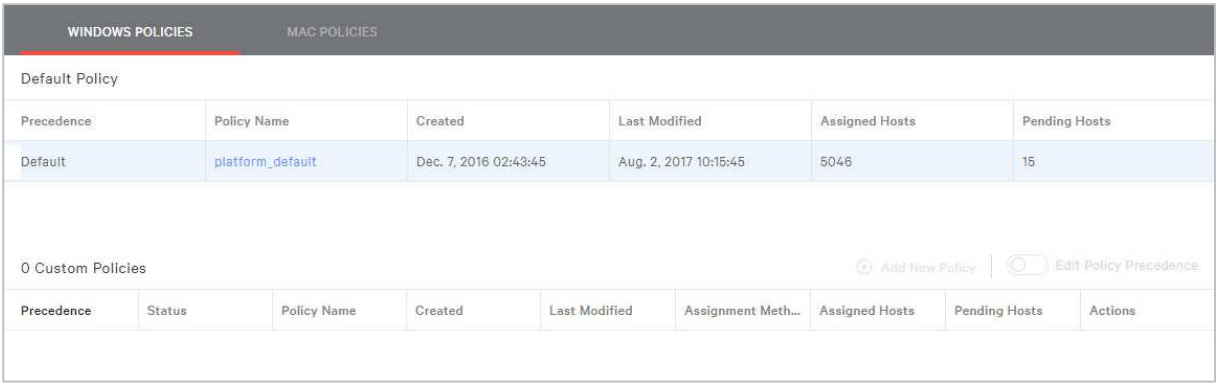
The *Hosts Dashboard* displays statistics relating to clients:



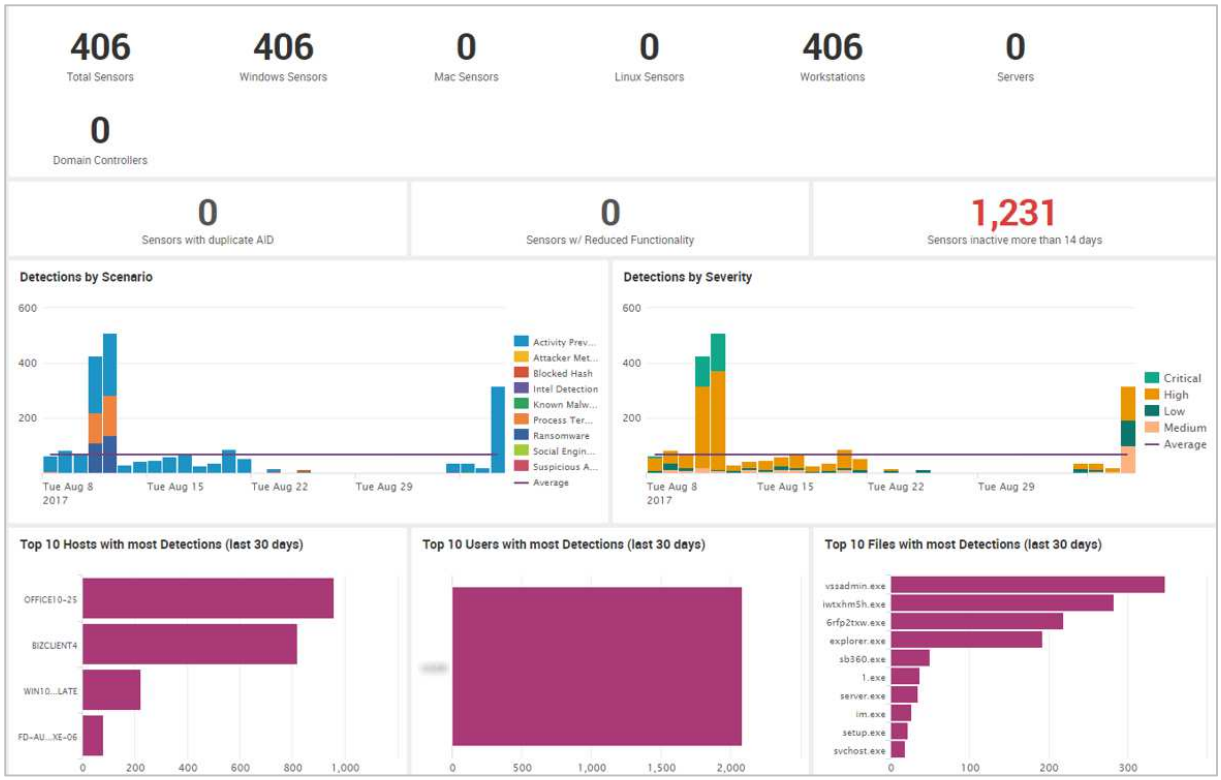
Hosts Management lists clients on the network:



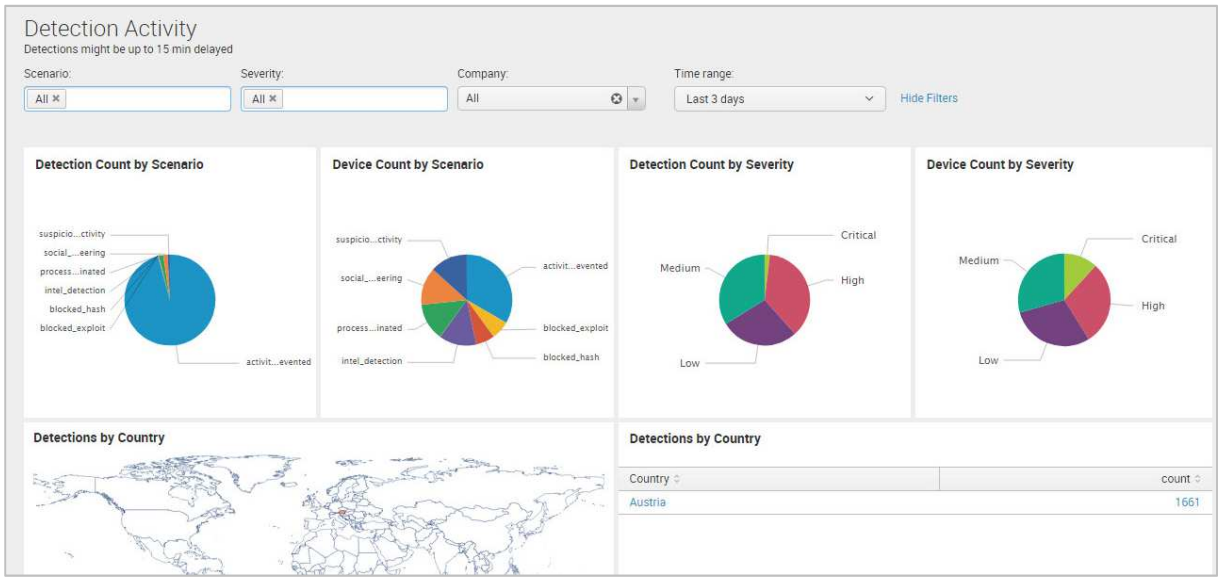
Configuration, Prevention Policies lists configuration policies to be applied to clients:



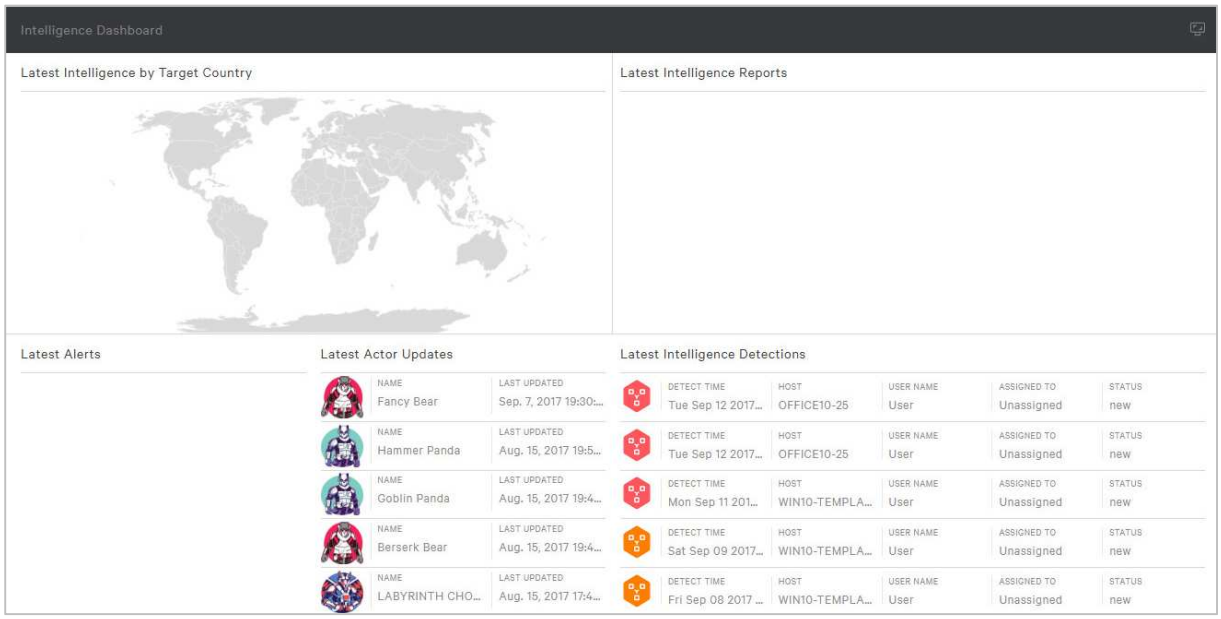
Under *Dashboards, Executive Summary* the admin can display a detailed breakdown of detections by scenario, severity, host or user:



Other *Dashboards* pages include *Detection Resolutions* and *Detection Activity* (shown below):



The *Intelligence Dashboard* provides information on the latest threats:



Controlling user access to the endpoint protection software

No GUI options for uninstall, command line uninstall can be setup to require administrator password.

Deployment methods for endpoint protection software

- Download the installer from console
- Use deployment and management tools like Microsoft SCCM to deploy the sensor
- Various command line parameter options allow for customized installation
- Once deployed, the product updates directly from the cloud and can be controlled via sensor groups

Windows client endpoint protection software

The client protection software registers in Windows Security Center as antivirus and antispyware.

The sensor can be configured from the Falcon Management Console to enable end user notifications, such as the malware alert shown below:

Emsisoft Enterprise Console

Overview

Product version reviewed

Emsisoft Enterprise Console 2017.7.0.3153
Emsisoft Anti-Malware 2017.7.0.7838

Windows operating systems supported

Management Console
Windows 7, 8.1, 10; Windows Server 2008/R2, 2012/R2

Endpoint Protection Software
Clients: Windows 7, 8, 10
Servers: Windows Server 2008 R2, 2012, 2012 R2

In our test, Emsisoft Anti-Malware endpoint protection software worked flawlessly on Windows Server 2016. The Emsisoft Enterprise Console can be run on a variety of other Windows Server and Windows client systems, and a version compatible with Server 2016 is expected in a future release.

About the product

Emsisoft Enterprise Console is a server-based management console that can be used to manage Windows client and server computers in a business network.

EDR features

Emsisoft Anti-Malware does not include EDR as such, but has a behaviour blocker with forensic logging.

Product information on vendor's website

https://www.emsisoft.com/en/software/enterprise/

Online support

https://www.emsisoft.com/en/support/contact/

Summary

The console has a very clean modern design, and the sensibly organised tabs along the top of the window make navigation very straightforward. In our test, we noted that commands are relayed from the console to the clients in a matter of seconds. With a little help from the excellent manual, the endpoint protection software is quick and easy to deploy, and provides a familiar GUI that lets users carry out everyday tasks.

Tips for administrators

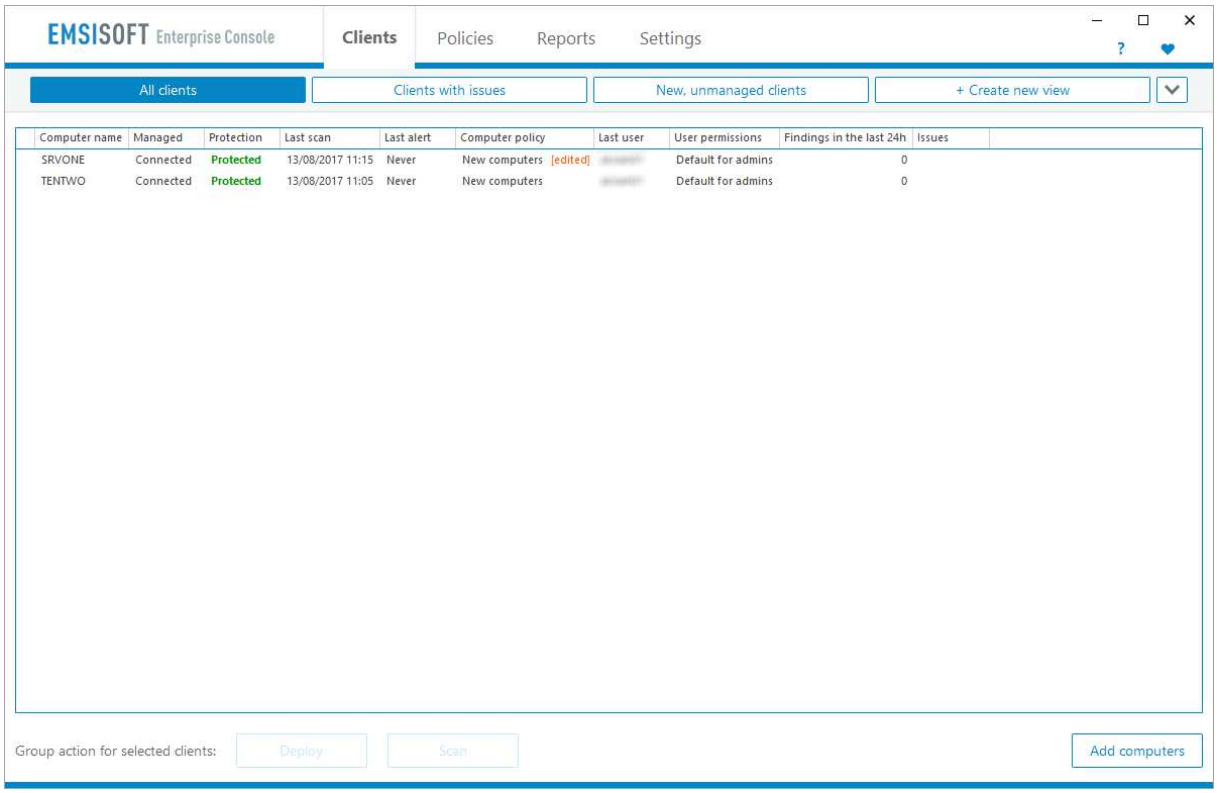
Emsisoft provide configuration scripts for client and server machines that make it very easy to prepare computers for remote installation. Details of where to find these scripts and how to use them can be found in the deployment section of the user guide.

Management Console

Installation and configuration

The console is installed by running a simple installer file on the server.

Layout



The console is navigated by a row of tabs along the top of the window, these being *Clients*, *Policies*, *Reports*, and *Settings*. Each page has a number of sub-tabs.

Deployment methods for endpoint protection software

- Push installation from console
- Running installation package from network share/USB device
- Via the Emsisoft Anti-Malware client software

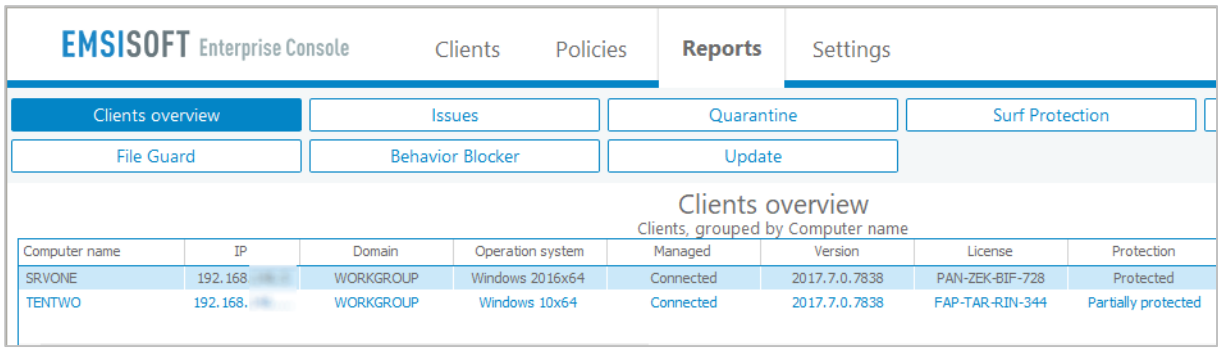
Monitoring the network

Status and alerts

These are shown on the *Clients* (home) page of the console, as in the screenshot above.

Program version

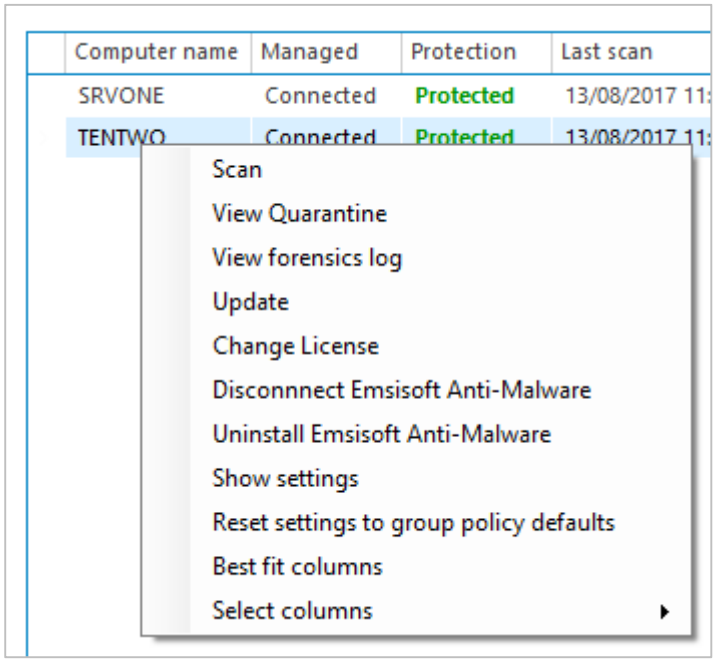
This can be found on the *Reports* tab, *Clients overview* sub-tab:



Managing the network

Scanning, scheduling scans, updates and removing devices from the console

Selecting one or more computers from the *Clients* page and right-clicking displays a context menu, from which the admin can run scans and updates, or disconnect/uninstall the endpoint protection software:

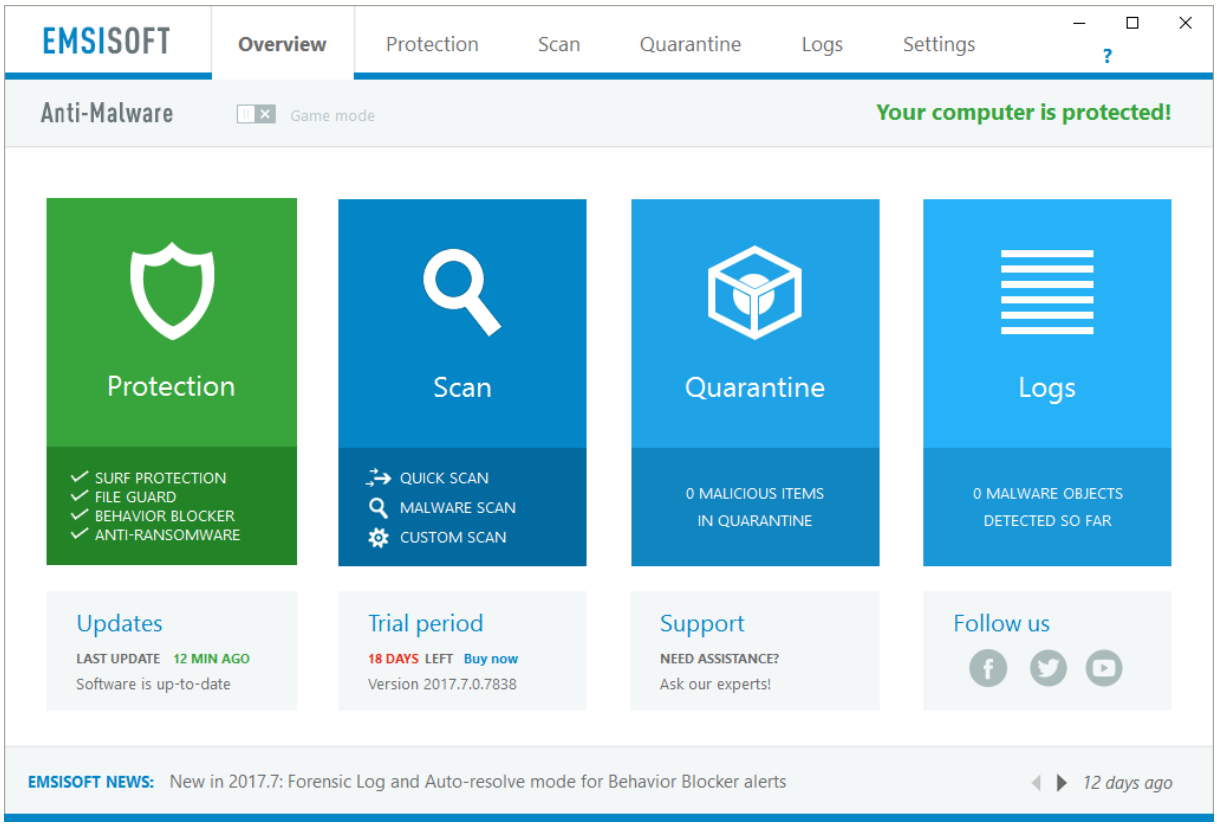


Controlling user access to the endpoint protection software

By default, users with Windows standard user accounts cannot reconfigure the product or disable protection. Custom user permissions can be configured in Policies in groups or based on AD permissions.

Windows client endpoint protection software

This is identical to the consumer version of Emsisoft Anti-Malware, the modern GUI included:



Tasks available to users

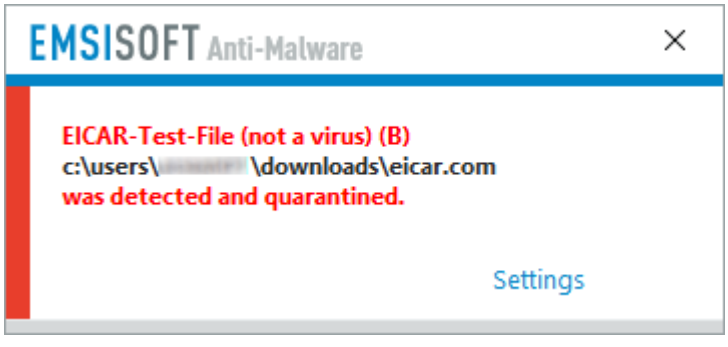
Users can run scans and updates from the user interface.

Windows Security Center/Windows Defender

Emsisoft Anti-Malware registers as the antivirus program in Windows Security Center. Windows Defender is disabled.

Alerts

If the EICAR test file is downloaded, the alert below is shown:



No user action is required. The alert closes after about 10 seconds.

If real-time protection is disabled, the *Protection* tile in the main window changes to show an alert:

Clicking on the disabled component allows the user to reactivate it.

Windows Server endpoint protection software

This can be regarded as identical to the client software.

Endgame Protection Platform

Overview

Product version reviewed

Endgame Protection Platform release version 2.4.2 which contains:

- Endgame Management Platform (cloud hosted) version 2.4.2
- Endgame sensor version 2.4.6

Windows operating systems supported

Clients: Windows 7, 8.1, 10 (32 and 64-bit)
Servers: Windows Server 2008 R2, 2012/R2, 2016 (32 and 64-bit)

About the product

Endgame uses an on-premise or cloud-based console and a single agent to manage prevention, detection and response, and threat hunting for Windows and Linux servers and clients. Support for Mac OS and Solaris is scheduled to be added to the product in Q1 2018.

EDR features

With regard to EDR features, Endgame state the following: *"Endgame's EDR capability continuously collects, enriches, encrypts, and stores endpoint telemetry data called ThreatFlow™. ThreatFlow™ collects event data for process execution, network communication including Netflow, DNS, File, Registry, various logon and other security events. Endgame Artemis®, powered by natural language understanding (NLU) technology, allows for access to ThreatFlow™ and facilitates root-cause analysis, triage, and response actions for every alert. A flexible two-way API can also be used to access data and respond. Threat hunting allows users to execute investigations across endpoints and identify threats, including embedded malware, injected code, malicious persistence, and other indicators of breach"*.

Product information on vendor's website

https://www.endgame.com/

Online support

https://www.endgame.com/company/customer-support

Summary

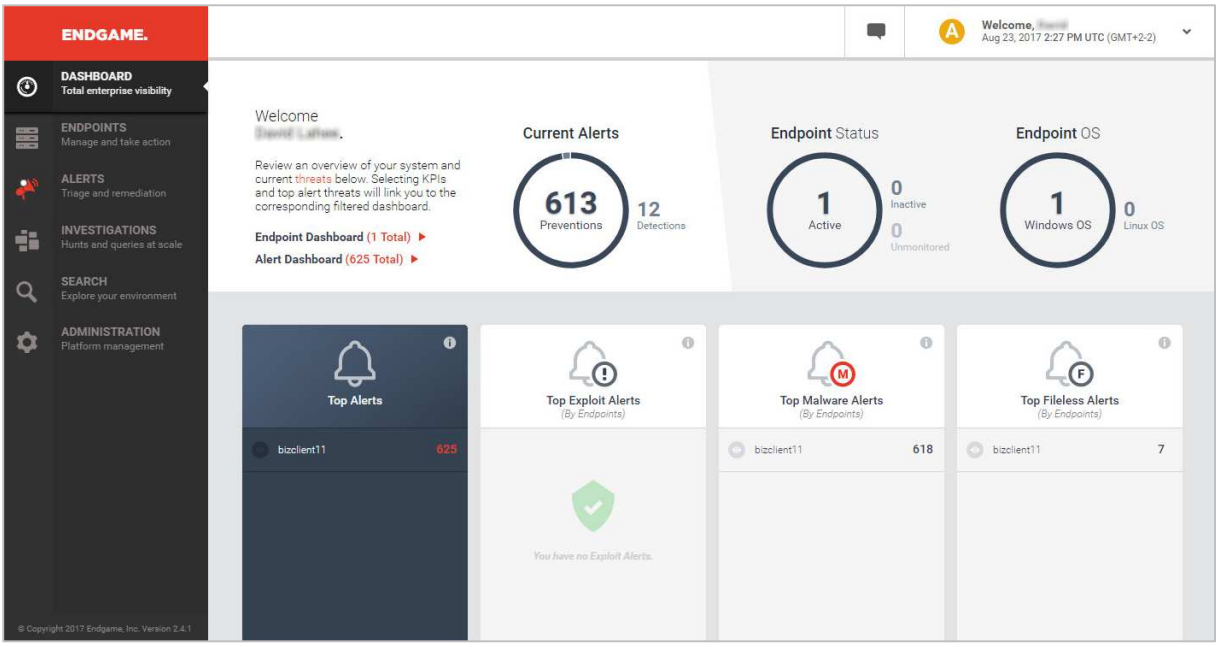
The nature of the product and its investigative capabilities mean that it will require some learning on the part of the administrator. However, we feel that the console design makes this as easy as possible, being very clean and well laid out, with familiar items such as status display and list of endpoints made very accessible. Easy navigation assists with the exploration of new features. The product is probably better suited to businesses large enough to have their own IT department.

Management Console

Installation and configuration

We used a cloud-based console in our test, so no installation was required. An on-premises deployment of the console is also available.

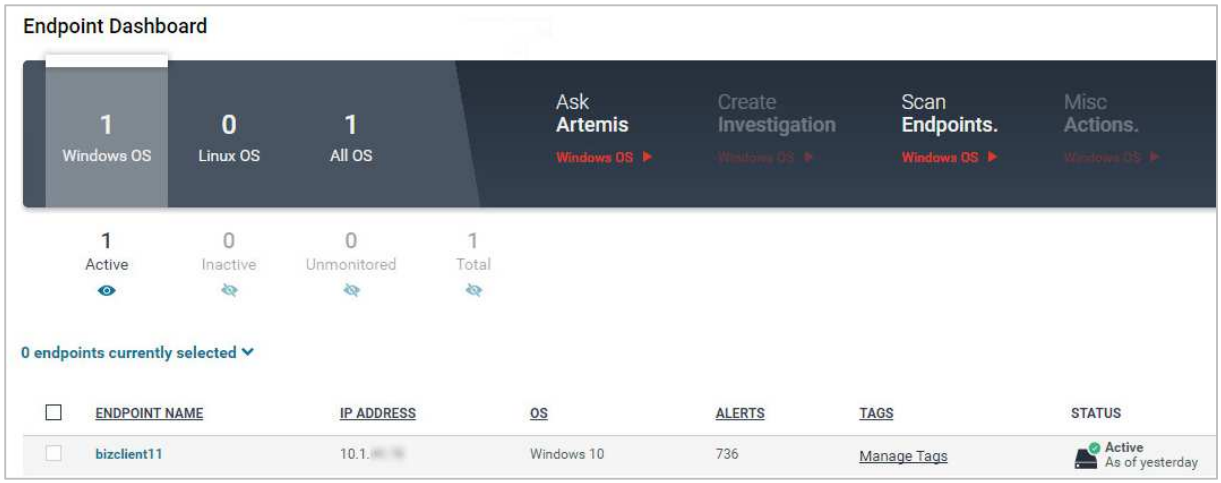
Layout and functionality



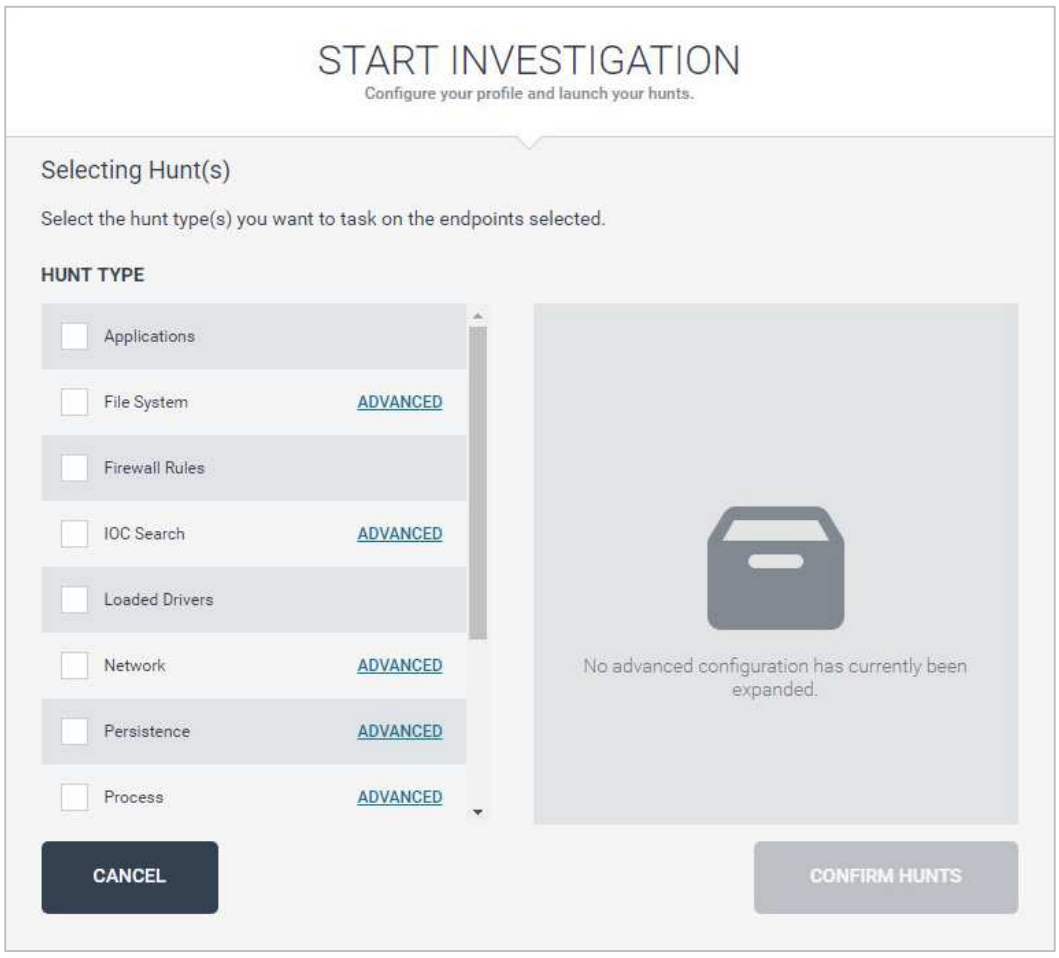
The console is navigated via a left-hand menu column, with the items *Dashboard, Endpoints, Alerts, Investigations, Search* and *Administration*.

Dashboard provides an overview of the system security status, as shown in the screenshot above. This displays the number of current alerts, along with *Endpoint Status* (active, inactive and unmonitored), as doughnut charts in the upper half of the page. The lower part of the page provides a breakdown of endpoints with the most alerts under *Top Exploit Alerts, Top Malware Alerts* and *Top Fileless Alerts*. Clicking on any of the doughnut charts opens an appropriate details page; for example, clicking on the hostname of the client at the top of the *Top Fileless Alerts* box opens a search query page displaying all the alerts of that type affecting the client in question.

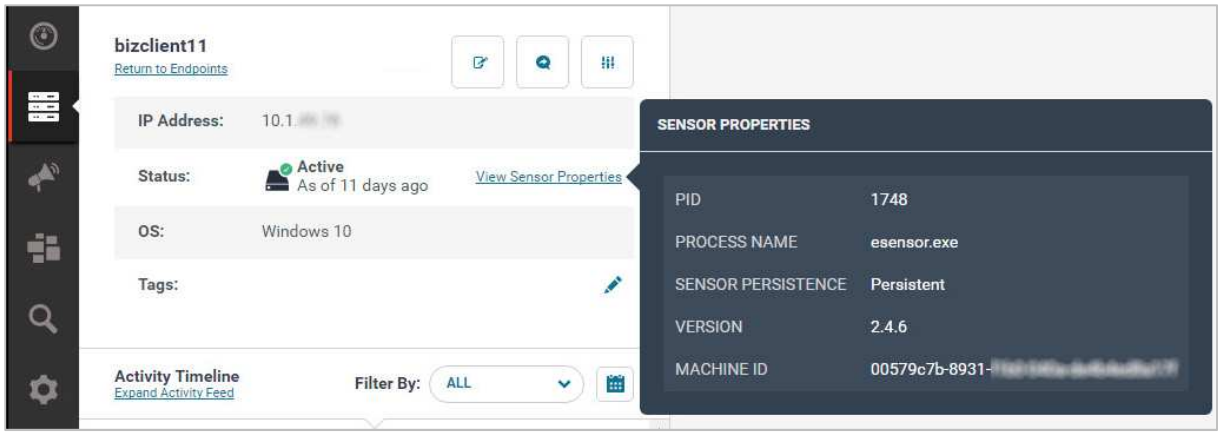
Clicking *Endpoints* in the console menu column displays a list of clients, which can are grouped by OS (currently Windows or Linux with Mac and Solaris support planned for Q1 2018):



The main menu bar at the top of the page contains a number of buttons for tasks that can be carried out on selected clients. *Ask Artemis* allows the admin to ask simple questions in plain English. For example, "Show me process lineage for evil.exe". Other questions include searches for process executions, network connections, DNS Queries or user events for groups of clients or specific clients. *Create Investigation* starts collection and analytics for specific items such as applications, firewall rules, loaded drivers, persistent software, which can then be easily inspected via the console:



Clicking on the hostname of an individual client (*Endpoint Name*) displays the details for that client. The *View Sensor Properties* link displays additional information about the sensor (Endgame agent):



Scan Endpoints should be regarded as a means of discovering clients prior to installing the Endgame agent on them, as opposed to a malware scan. Clicking *Miscellaneous Actions* opens a submenu of further tasks:

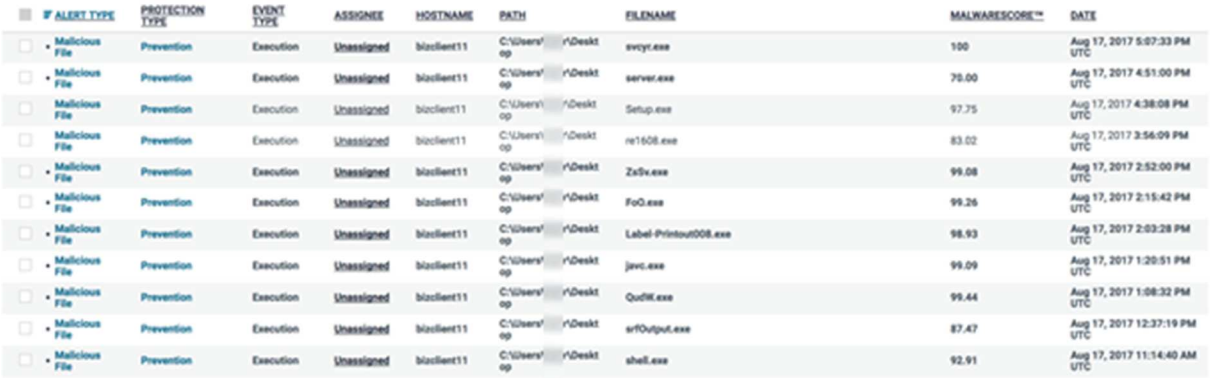
Respond lets the admin choose a variety of reactions to an alert:

Tag allows the administrator to add any kind of text description to allow the client(s) concerned to be found and sorted in search queries.

The *Alerts* tab shows current alerts from all clients. These can be sorted according to *Alert Type, Protection Type, Event Type, Assignee, IP Address, Hostname or Date*:

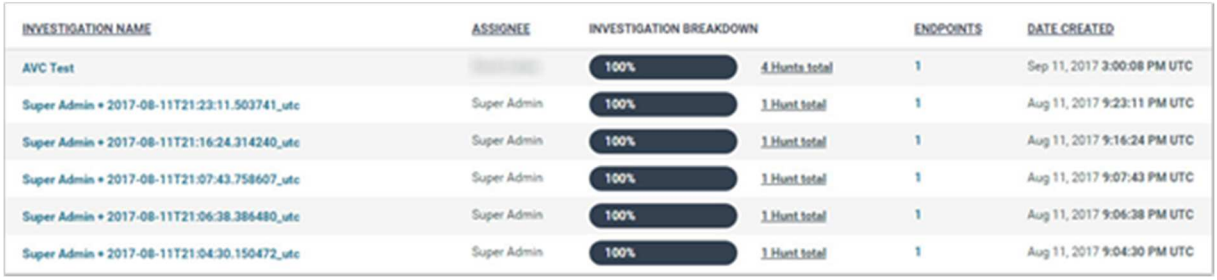
ALERT TYPE	PROTECTION TYPE	EVENT TYPE	ASSIGNEE	IP ADDRESS	HOSTNAME	DATE
• Malicious File	Prevention	Execution	Unassigned	10.1.	bizclient11	Aug 26, 2017 4:53:36 PM UTC
• Malicious File	Prevention	Execution	Unassigned	10.1.	bizclient11	Aug 26, 2017 4:04:28 PM UTC
• Malicious File	Prevention	Execution	Unassigned	10.1.	bizclient11	Aug 26, 2017 3:30:05 PM UTC
• Malicious File	Prevention	Execution	Unassigned	10.1.	bizclient11	Aug 26, 2017 2:50:13 PM UTC
• Malicious File	Prevention	Execution	Unassigned	10.1.	bizclient11	Aug 26, 2017 1:08:26 PM UTC
• Malicious File	Prevention	Execution	Unassigned	10.1.	bizclient11	Aug 26, 2017 12:29:49 PM UTC
• Malicious File	Prevention	Execution	Unassigned	10.1.	bizclient11	Aug 26, 2017 10:41:40 AM UTC
• Malicious File	Prevention	Execution	Unassigned	10.1.	bizclient11	Aug 26, 2017 10:01:06 AM UTC
• Malicious File	Prevention	Execution	Unassigned	10.1.	bizclient11	Aug 26, 2017 9:44:21 AM UTC
• Process Injection	Prevention	Shellcode Injection	Unassigned	10.1.	bizclient11	Aug 26, 2017 9:34:28 AM UTC

Selecting an alert type provides details most commonly used for rapid triage of each alert of that type. Columns can be clicked for further sorting, search, or aggregation of alerts.



ALERT TYPE	PROTECTION TYPE	EVENT TYPE	ASSIGNEE	HOSTNAME	PATH	FILENAME	MALWARESCORE™	DATE
• Malicious File	Prevention	Execution	Unassigned	bizclient11	C:\Users\ op	svcyr.exe	100	Aug 17, 2017 5:07:33 PM UTC
• Malicious File	Prevention	Execution	Unassigned	bizclient11	C:\Users\ op	server.exe	70.00	Aug 17, 2017 4:51:00 PM UTC
Malicious File	Prevention	Execution	Unassigned	bizclient11	C:\Users\ op	Setup.exe	97.75	Aug 17, 2017 4:38:08 PM UTC
Malicious File	Prevention	Execution	Unassigned	bizclient11	C:\Users\ op	re1608.exe	83.02	Aug 17, 2017 3:56:09 PM UTC
• Malicious File	Prevention	Execution	Unassigned	bizclient11	C:\Users\ op	ZaSv.exe	99.08	Aug 17, 2017 2:52:00 PM UTC
• Malicious File	Prevention	Execution	Unassigned	bizclient11	C:\Users\ op	FoO.exe	99.26	Aug 17, 2017 2:15:42 PM UTC
• Malicious File	Prevention	Execution	Unassigned	bizclient11	C:\Users\ op	Label-Printout008.exe	98.93	Aug 17, 2017 2:03:28 PM UTC
• Malicious File	Prevention	Execution	Unassigned	bizclient11	C:\Users\ op	javc.exe	99.09	Aug 17, 2017 1:20:51 PM UTC
• Malicious File	Prevention	Execution	Unassigned	bizclient11	C:\Users\ op	QuiW.exe	99.44	Aug 17, 2017 1:08:32 PM UTC
• Malicious File	Prevention	Execution	Unassigned	bizclient11	C:\Users\ op	srfOutput.exe	87.47	Aug 17, 2017 12:37:19 PM UTC
• Malicious File	Prevention	Execution	Unassigned	bizclient11	C:\Users\ op	shell.exe	92.91	Aug 17, 2017 11:14:40 AM UTC

The *Investigations* page of the console shows data searches that have been created previously:



INVESTIGATION NAME	ASSIGNEE	INVESTIGATION BREAKDOWN		ENDPOINTS	DATE CREATED
AVC Test		100%	4 Hunts total	1	Sep 11, 2017 3:00:08 PM UTC
Super Admin • 2017-08-11T21:23:11.503741_utc	Super Admin	100%	1 Hunt total	1	Aug 11, 2017 9:23:11 PM UTC
Super Admin • 2017-08-11T21:16:24.314240_utc	Super Admin	100%	1 Hunt total	1	Aug 11, 2017 9:16:24 PM UTC
Super Admin • 2017-08-11T21:07:43.758607_utc	Super Admin	100%	1 Hunt total	1	Aug 11, 2017 9:07:43 PM UTC
Super Admin • 2017-08-11T21:06:38.386480_utc	Super Admin	100%	1 Hunt total	1	Aug 11, 2017 9:06:38 PM UTC
Super Admin • 2017-08-11T21:04:30.150472_utc	Super Admin	100%	1 Hunt total	1	Aug 11, 2017 9:04:30 PM UTC

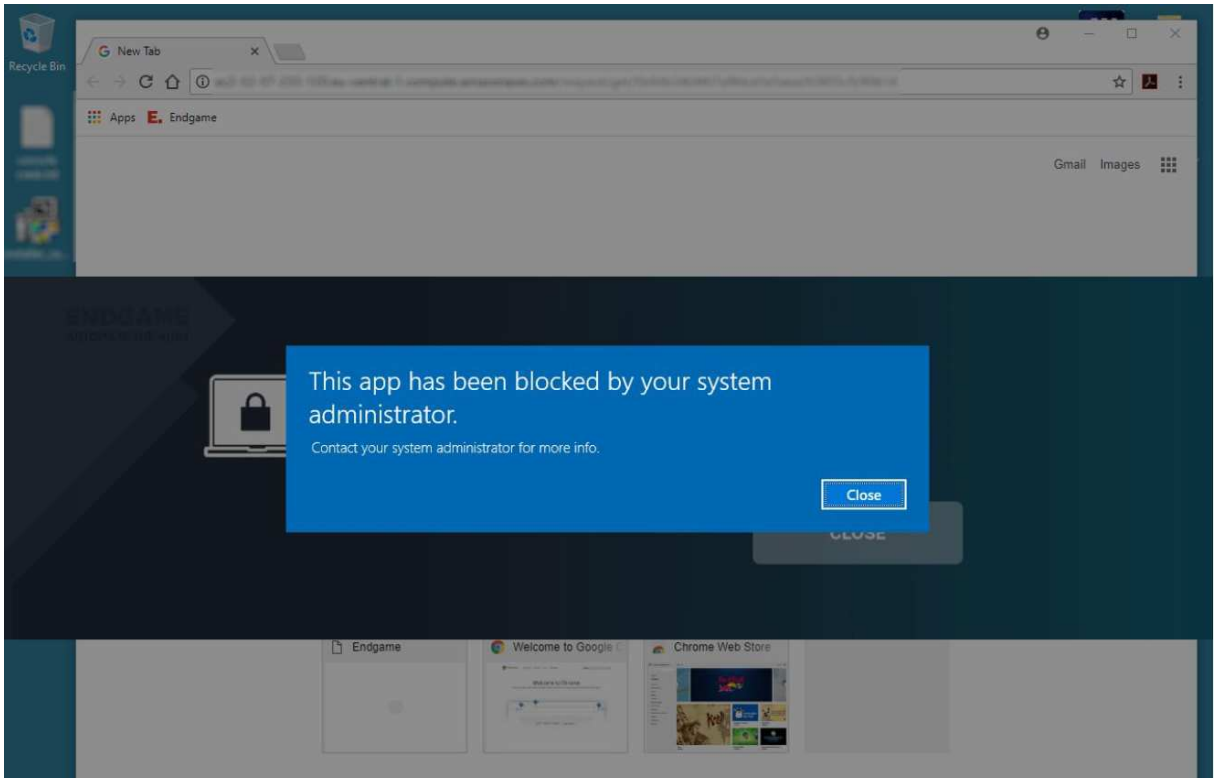
The *Administration* page allows users, alerts, whitelists etc. to be managed.

Deployment methods for endpoint agent

- Download installer from console and run
- Remote push installation via the console using domain credentials

Windows client endpoint protection software

There is no visible interface to the client software, although an Endgame alert is shown when a malicious file is blocked. In the screenshot below, the Endgame alert is partially covered by a Windows alert.



Windows Server endpoint protection software

This can be regarded as identical to the client software.

ESET Remote Administrator

Overview

Product version reviewed

ESET Remote Administrator Server 6.5.522.0
ESET Remote Administrator Console 6.5.388.0
ESET File Security for Microsoft Windows Server 6.5.12010.0
ESET Endpoint Security 6.5.2107.1

Windows operating systems supported

Administration console

Windows Server 2003 x64, 2008/R2, 2012/R2, 2016; Windows 7, 8, 8.1, 10

Endpoint protection software

ESET Endpoint Security: Windows XP, Vista, 7, 8, 8.1, 10
ESET File Security: Windows Server 2003, 2008/R2, 2012/R2, 2016; Windows Small Business Server 2003/R2, 2008, 2011

About the product

ESET Remote Administrator is available as a server-based console for Windows and Linux OS, as a virtual appliance for VMware, Oracle and Microsoft Hyper-V virtualisation systems, or as a preconfigured VM in Microsoft Azure.

EDR features

With regard to EDR features, ESET state the following: *"ESET make a standalone EDR product called ESET Enterprise Inspector[2], with an independent agent integrated with ESET Remote Administrator. It collects endpoint data in real time, and matches it against a rule set to automatically detect suspicious activities. The admin can see and inspect every program being executed in the company network and check its characteristics and operations performed by it. He/she can then decide whether or not to allow the process to run in the company network. Analysis of the parent process can how determine how a suspicious process started."*

Product information on vendor's website

https://www.eset.com/int/business/remote-management/remote-administrator/

Online support

http://support.eset.com/?segment=business

Summary

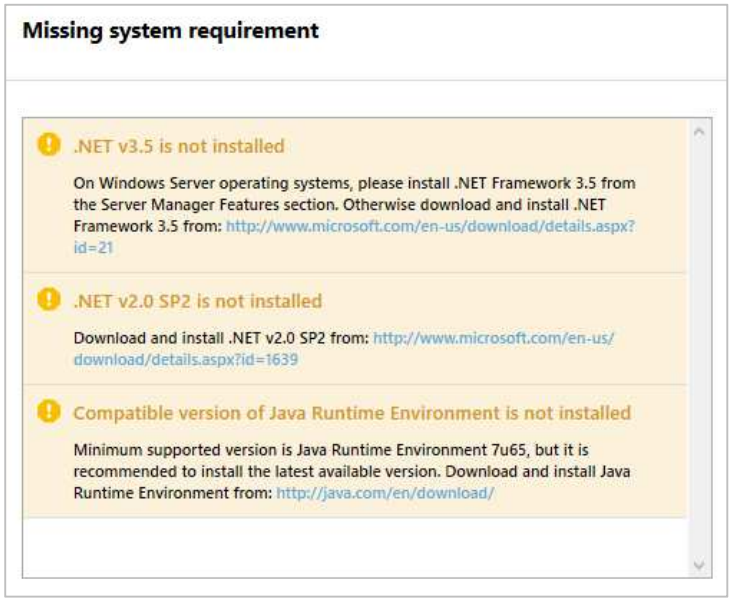
ESET Remote Administrator is a powerful console that can easily cope with large-scale corporate networks. Its design and layout make basic everyday tasks easy to find. This, combined with very familiar client software and a range of excellent help features, means it could be employed successfully in small businesses too.

[2] https://www.eset.com/int/business/remote-management/enterprise-inspector/

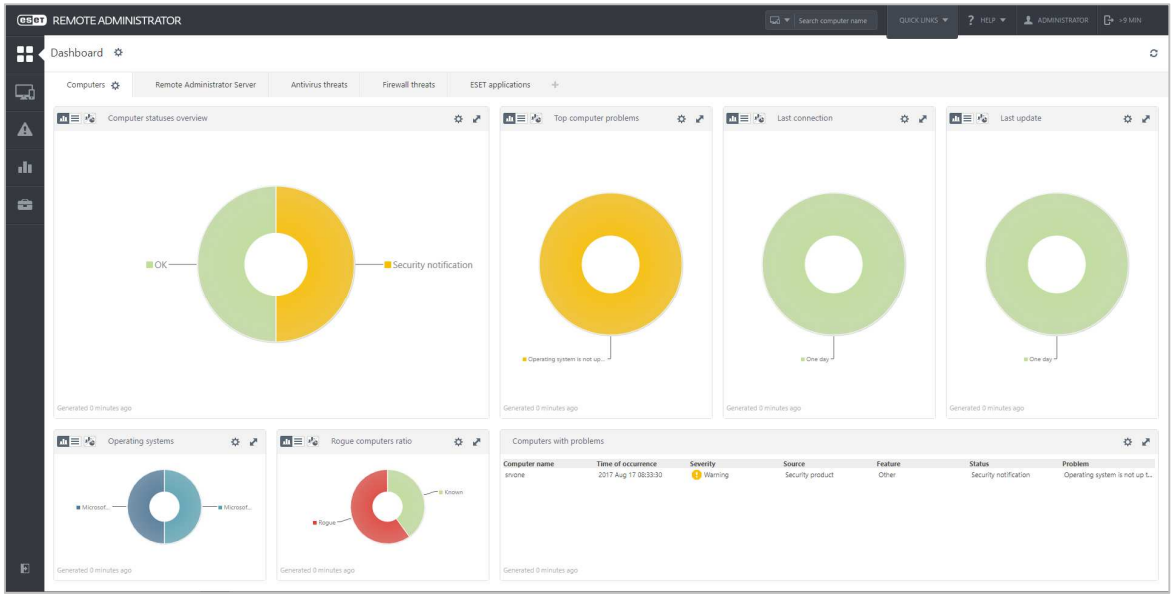
Management Console

Installation and configuration

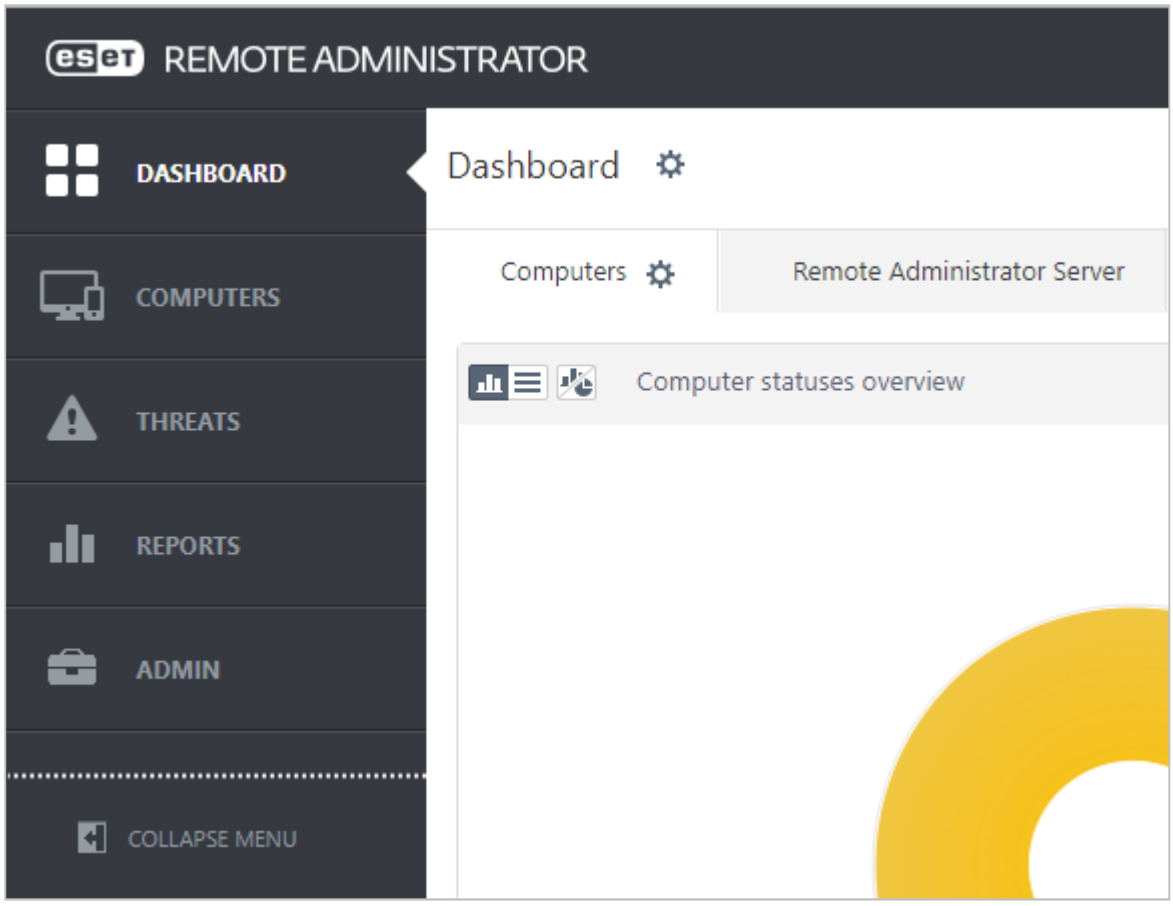
There are two components to ESET Remote Administrator, the server (functionality) and console (user interface). These can be installed separately – the console can connect to a server running on a different machine – or together with an all-in-one installer. The setup wizard notifies the admin of any additional components required, with convenient links to download them from:



Layout



The console is navigated by means of a menu bar on the left-hand side. This can be expanded to display the names of the links, or collapsed to save space.



The *Dashboard* (home) page shows an overview of the state of the network, while *Admin* allows items such as users, installation packages, licences and certificates to be managed.

Deployment methods for endpoint protection software

- Sharing installation package via network share or removable device
- Remote push installation

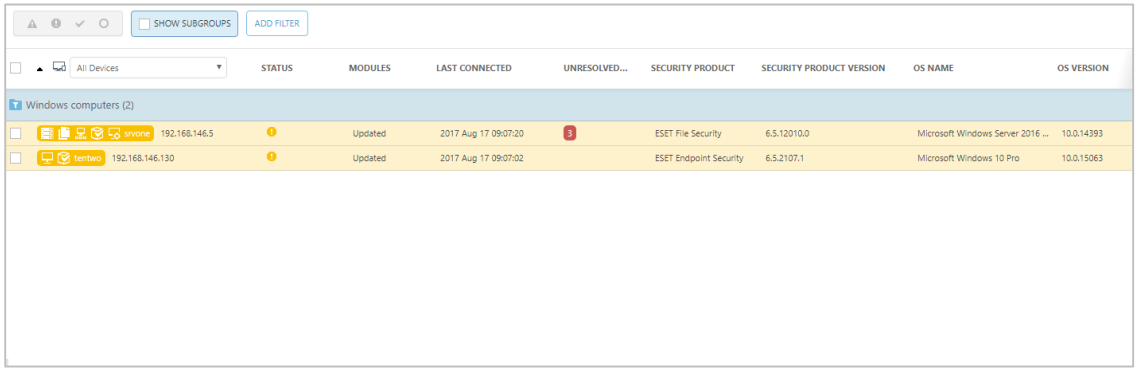
Monitoring the network

Status and alerts

These are shown on the *Dashboard* page, with various items including *Computer Status, Computer Problems, Operating Systems* and *Rogue Computers*, in the form of doughnut charts. The page can be customised by changing the items shown, size of the tile, and type of chart, among other things.

Program version

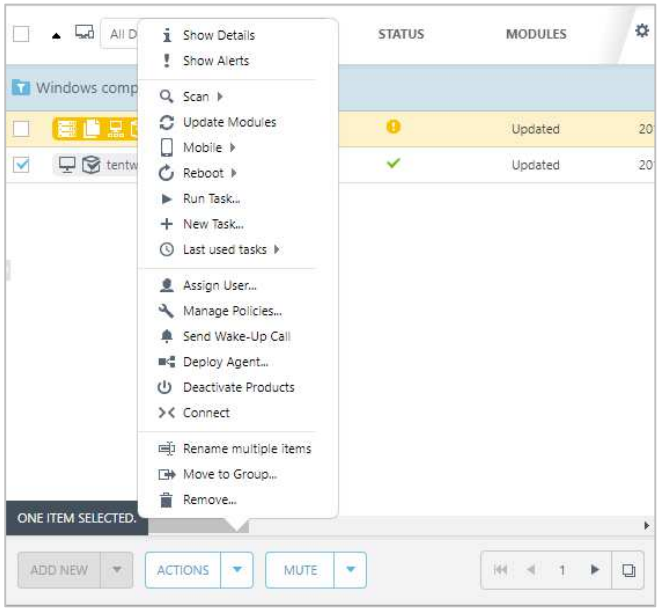
This is shown along with numerous other properties on the *Computers* page:



Managing the network

Scanning, scheduling scans, updates and removing devices from the console

A default scan can be run by selecting devices from the *Computers* page and selecting *Scan* from the *Actions* menu:



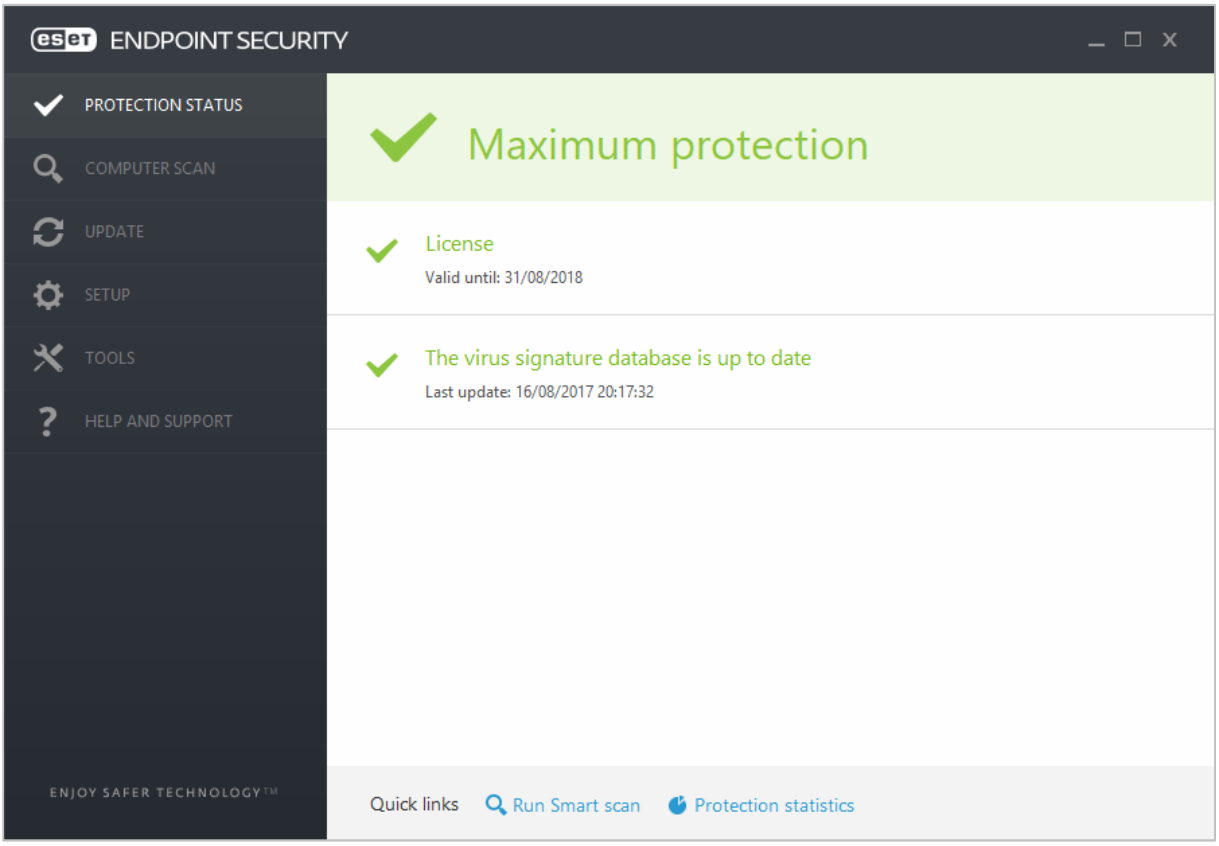
The same menu can be used to remove a device from the console, run an update (*Update* Modules) or run a scheduled scan by means of creating a task.

Controlling user access to the endpoint protection software

By default, users with standard user accounts cannot disable any protection features.

Windows client endpoint protection software

There is a full GUI, similar to a consumer antivirus program:



Tasks available to users

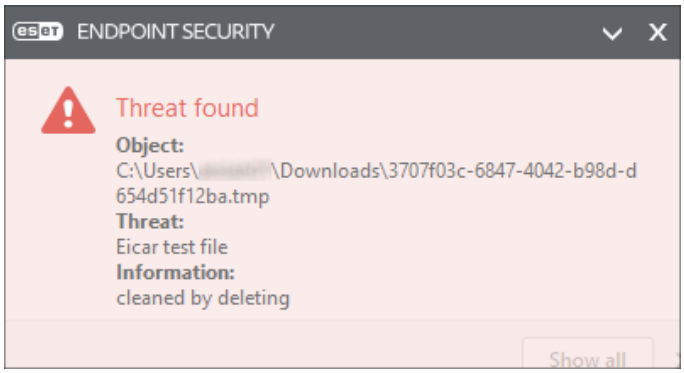
Users can run updates and a full range of scans from the GUI.

Windows Security Center/Windows Defender

ESET Endpoint Security registers in Windows Security Center as the antivirus and firewall programs. Windows Defender and Windows Firewall are disabled.

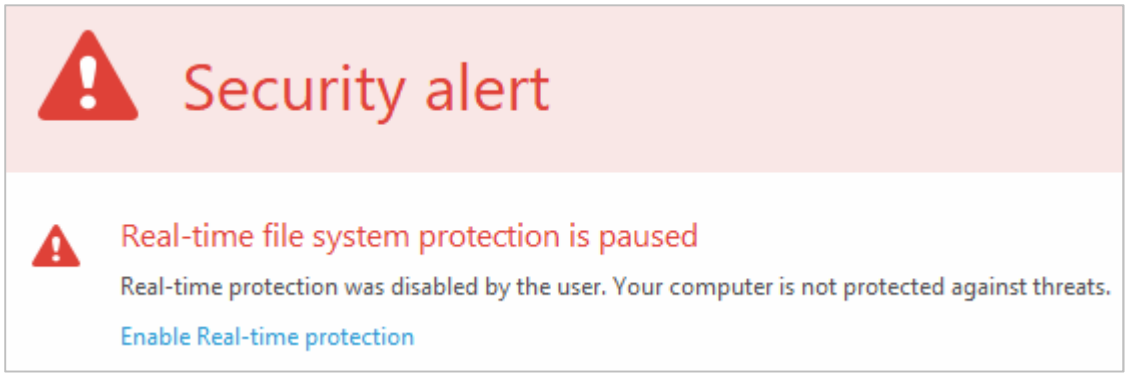
Alerts

If the EICAR test file is downloaded, the alert below is shown:



No user interaction is required. The alert closes after a few seconds.

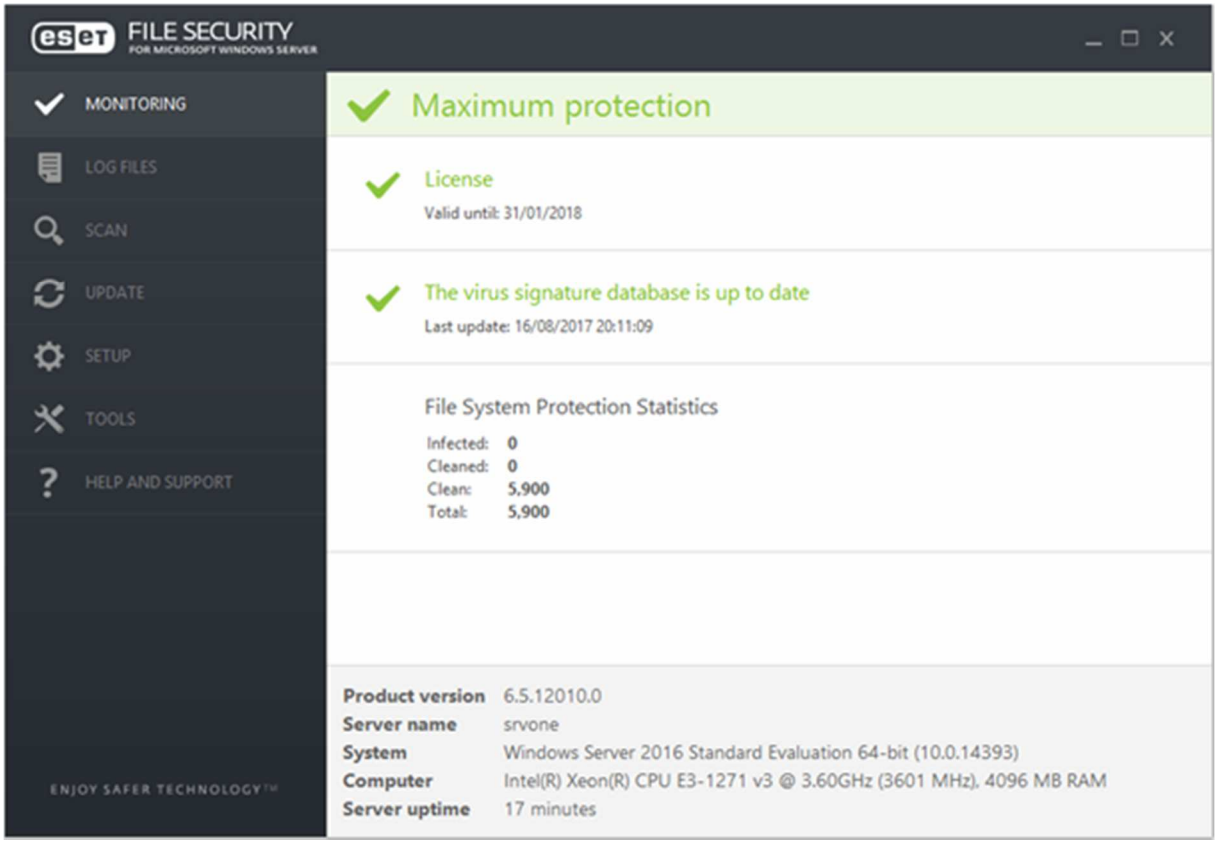
If real-time protection is disabled, the alert below is shown in the status section of the main program window:



The protection can be instantly reactivated by clicking *Enable Real-time protection*.

Windows Server endpoint protection software

This is very similar to the client software,although there are some differences on account of its server-based role. For example, the program relies on the Windows Server Firewall rather than installing the ESET firewall, and the interface includes an additional menu item for log files and a product information section at the bottom of the window.



FortiClient Enterprise Management Server

Overview

Product version reviewed

FortiClient Enterprise Management Server 1.2.1.0394
FortiClient endpoint protection 5.6.0.1075

Windows operating systems supported

Management console
Windows Server 2008 R2, 2012, 2012 R2, 2016

Endpoint protection
Clients: Windows 7, 8.1, 10
Servers: Windows Server 2008 R2, 2012, 2012 R2, 2016

About the product

FortiClient Enterprise Management Server is a server-based console used to manage endpoint protection software for Windows and Mac OS clients and Windows servers.

EDR features

With regard to EDR features, Fortinet state the following: *"A combination of Fortinet products may be used in concert to provide this functionality: FortiAnalyzer provides centralized network security logging and reporting for the Fortinet Security Fabric, for example collecting and providing analysis of logs for judgement from both FortiClient endpoints and FortiSandbox."*

Product information on vendor's website

https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiClient.pdf

Online support

https://support.fortinet.com/

Summary

FortiClient Enterprise Management Server is easy to install and very straightforward to navigate. It has the ability to manage multiple domains/workgroups, making it suitable for larger networks, although the simplicity of its layout means it could work well for smaller networks too. A comprehensive and detailed user manual is provided.[3]

We would advise administrators to consult the manual before undertaking deployment or other operations, as we did not always find using the console to be completely intuitive. For example, when creating an installation package, the admin has to deliberately add the antivirus and firewall components, which are not included by default. It is also necessary to ensure that these components are included in the default policy, and that this is assigned to all clients/client groups. To uninstall FortiClient endpoint protection software, the client computer has to be disconnected from the management console before the *Uninstall* option appears in its Control Panel.

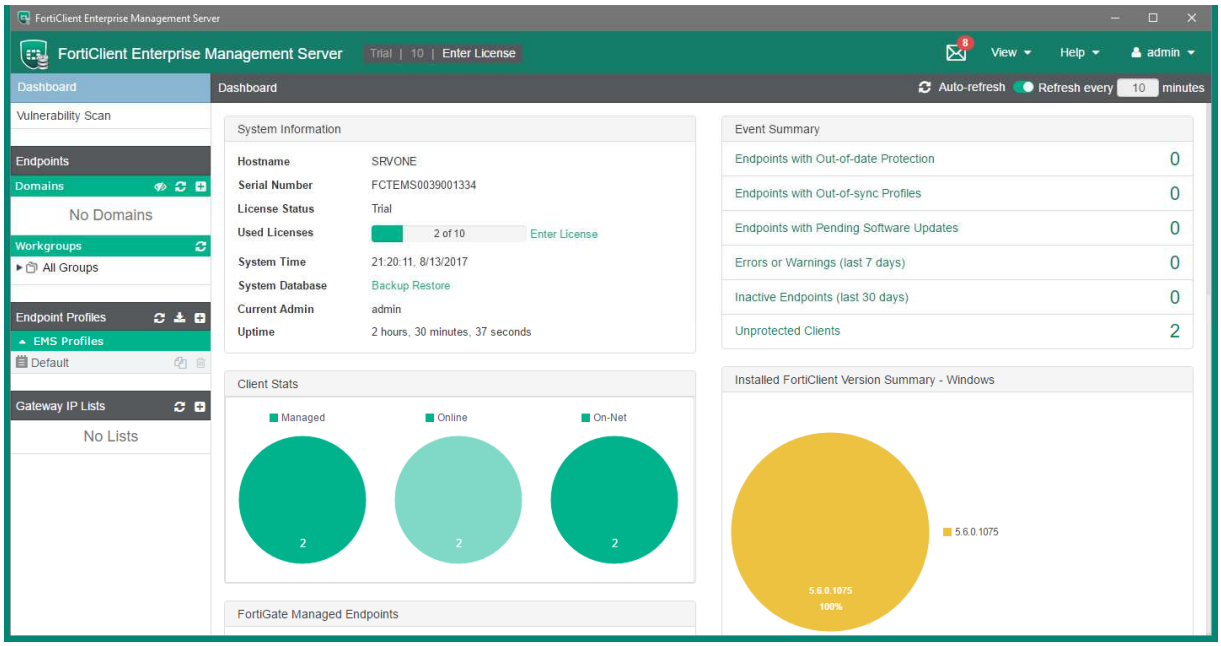
[3] http://docs.fortinet.com/uploaded/files/3269/forticlient-ems-v1.0.2-admin-guide.pdf

Management Console

Installation and configuration

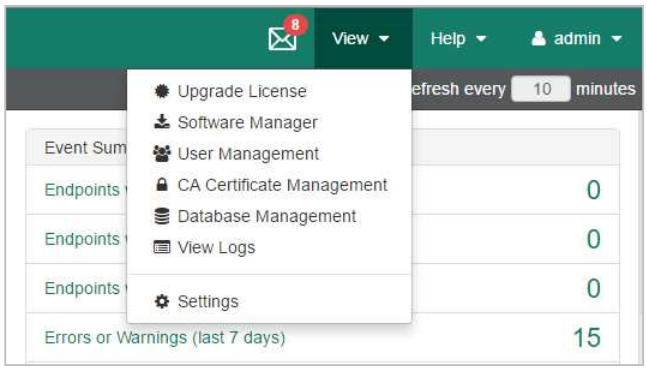
The console is installed by running the installer and completing a straightforward setup wizard.

Layout



The left-hand menu panel allows the admin to access network computers from *Endpoints*; these are grouped into *Domains* (Active Directory) and *Workgroups*. The same panel also shows *Endpoint Profiles*, i.e. configuration policies to be applied to managed computers. The *View* menu in the top right-hand corner of the window provides access to other important functions, such as logs, settings, and the

Software Manager:



Deployment methods for endpoint protection software

- Distributing installer file via network share or removable device
- Download from server via http

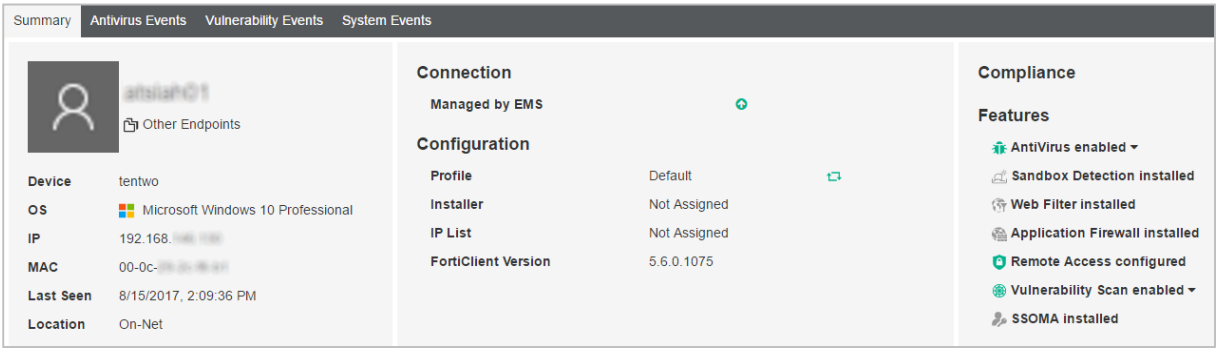
Monitoring the network

Status and alerts

These are shown on the *Dashboard* (home) page of the console.

Program version

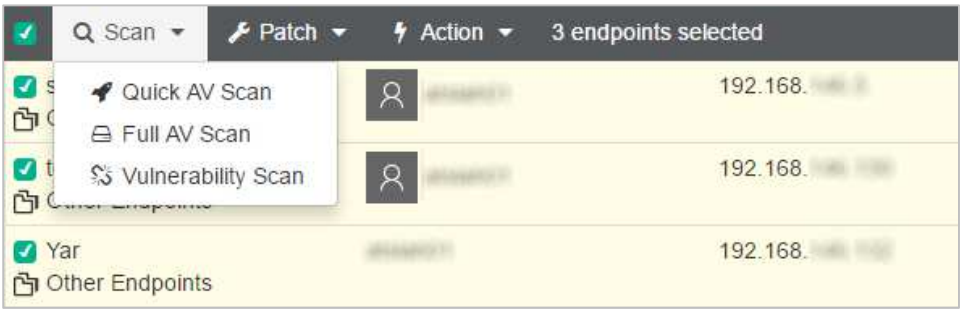
Percentages of computers using specific program versions are shown in the *Installed FortiClient Version Summary* pie chart on the *Dashboard* page. The version running on any individual device can be seen in that computer's details under *Endpoint Profiles*:



Managing the network

Scanning, scheduling scans, updates and removing devices from the console

To run a scan, the admin selects the relevant computer(s) from the appropriate group under *Endpoints*, clicks *Scan*, and the appropriate scan type from the drop-down menu:



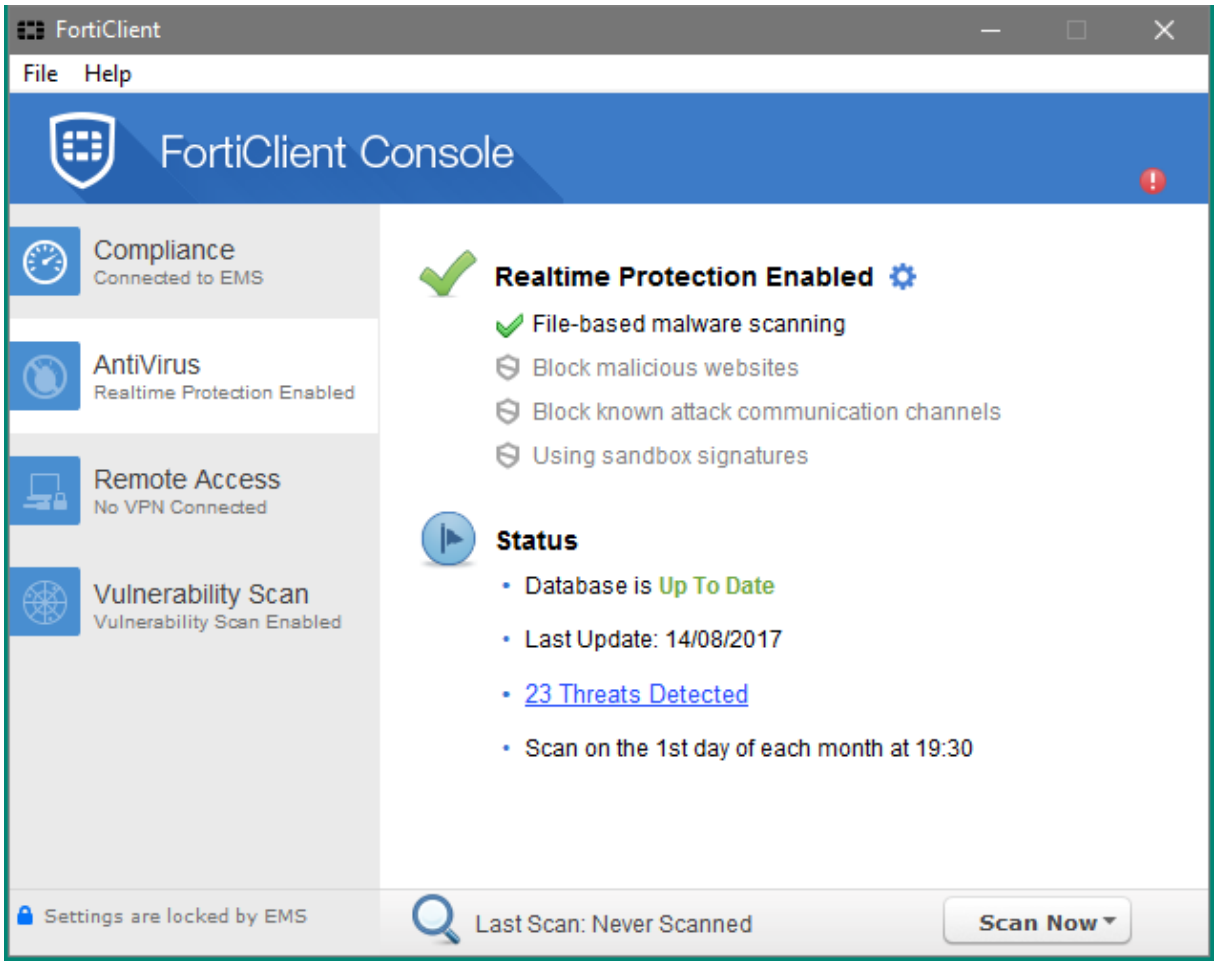
Updates can be run in similar fashion from the *Action* menu, which can also be used to remove devices from the console.

Controlling user access to the endpoint protection software

By design, client settings may only be changed from the console, so as to prevent accidental changes by end users.

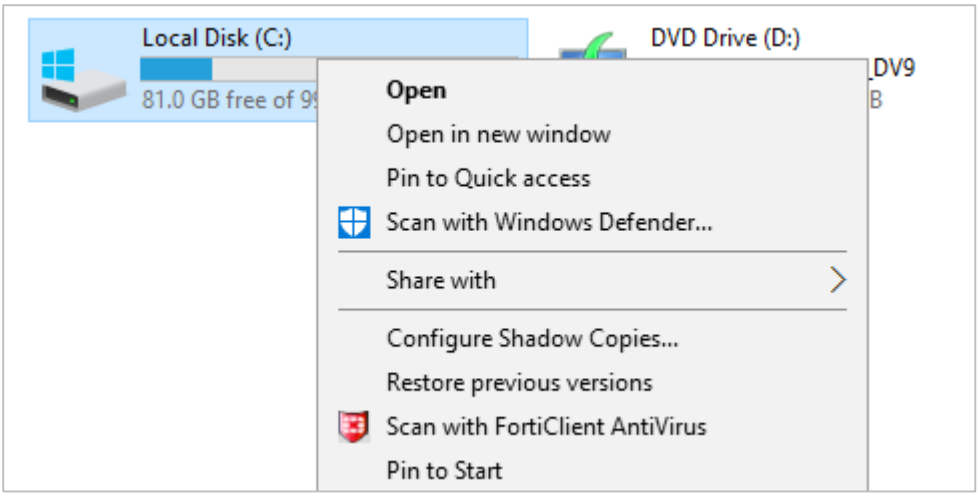
Windows client endpoint protection software

The *Antivirus* page of the FortiClient console shows endpoint status details:



Tasks available to users

Users can initiate a Quick, Full, Custom, or Removable Media scan from the program window, or scan drives, folders or files by right-clicking them and clicking *Scan with FortiClient AntiVirus* in the context menu:

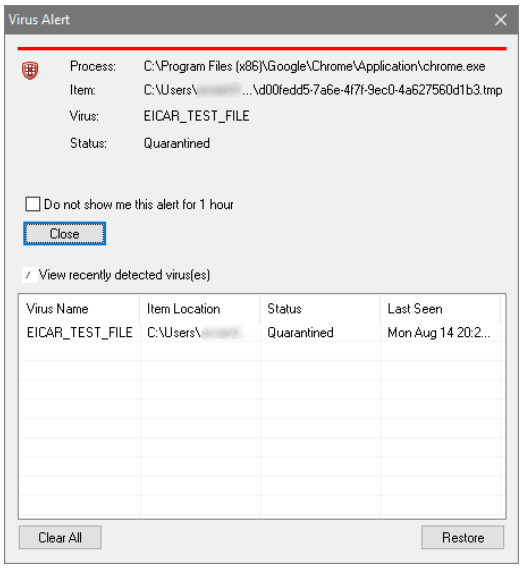


Windows Security Center/Windows Defender

FortiClient registers in Windows Security Center as the antivirus program, and Windows Defender is disabled. Fortinet describes the FortiClient Firewall module as an application layer firewall; that is to say, it monitors network traffic generated by applications. It is to be regarded as a supplement to Windows Firewall, not as a replacement for it. If it is installed and enabled, it does not deactivate Windows Firewall nor register in Windows Security Center as a system firewall.

Alerts

If the EICAR test file is downloaded, the alert below is shown:



No user action is required. The alert persists until closed.

If Realtime Protection is disabled by changing the profile being applied to the endpoint from within the EMS console, the text and graphic of the status display change to show this:

Protection using antivirus signatures can only be reactivated by enabling Realtime Protection the EMS console. Similarly, for other security features such as webfiltering and application firewall, if the feature is disabled in the profile, the FortiClient console will reflect this change as soon as the updated profile is received and applied from EMS.

Windows Server endpoint protection software

This is identical to the client software.

F-Secure Protection Service for Business

Overview

Product version reviewed

F-Secure PSB Workstation Security 12.0.1
F-Secure PSB Server Security 12.10

Windows operating systems supported

Clients: At the time of writing, system requirements for Workstation Security were shown on the F-Secure website as Windows Vista, 7, and 8/8.1, although the software worked flawlessly under Windows 10 in our test.[4]

Servers: Windows Server 2008/R2, 2012/R2, 2016; Windows Small Business Server 2008, 2011

About the product

F-Secure Protection Service for Business uses a cloud-based console to manage Windows and Mac OS clients, and Windows Servers.

EDR features

With regard to EDR, F-Secure say they are to release an EDR product during 2018.

Product information on vendor's website

https://www.f-secure.com/en/web/business_global/protection-service-for-business

Online support

https://emea.psb.f-secure.com/#/c273764/support

Summary

F-Secure Protection Service for Business impressed us with its very clear and intuitive console design, which makes finding and using everyday functions very straightforward. Client software is easy to install and use. Overall, the package is very user-friendly and consequently ideal for small businesses that do not have a full-time IT administrator.

Suggestions for improvement

We feel that a simple and effective means of preventing users disabling protection would be a valuable addition.

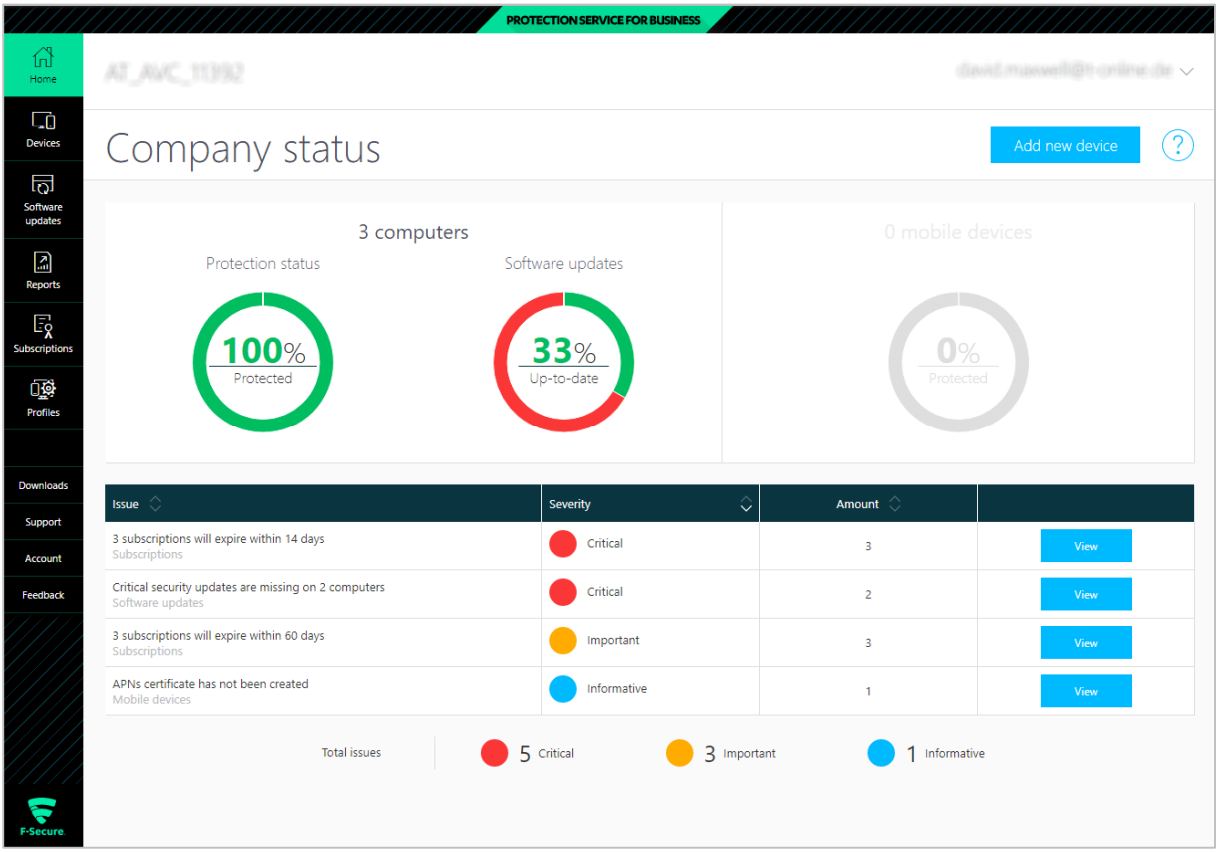
[4] https://community.f-secure.com/t5/Business/What-are-the-system-requirements/ta-p/71601

Management Console

Setup

The console is cloud-based and so does not require installation.

Layout



There is a single menu bar down the left-hand side of the page, allowing the admin to navigate the console's functions easily.

Home provides a detailed status display

Devices displays the computers on the network and allows management functions such as scans, updates and policy management

Reports provides logs of malware detections etc.

Profiles lets the admin create and apply configuration policies

Downloads provides installation packages for the different operating systems supported

Deployment methods for endpoint protection software

- Download from console and install directly on local computer
- Email installation link to users

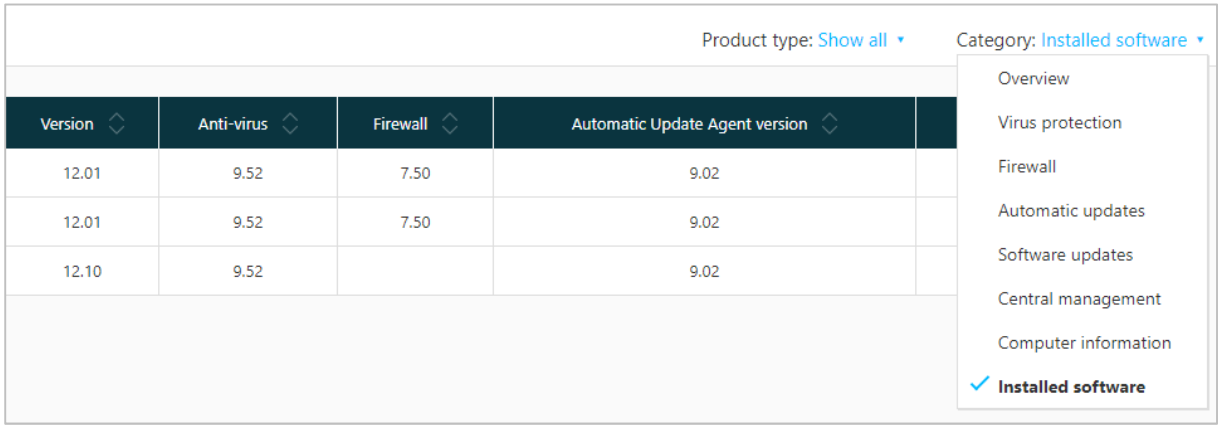
Monitoring the network

Status and alerts

These are shown on the home page of the console, with separate displays for protection status, software updates, subscriptions due to expire, and critical security updates.

Program version

This can be found by clicking on *Devices* in the menu column, and selecting *Installed software* from the *Category* menu:



Managing the network

Scanning, scheduling scans, updates and removing devices from the console

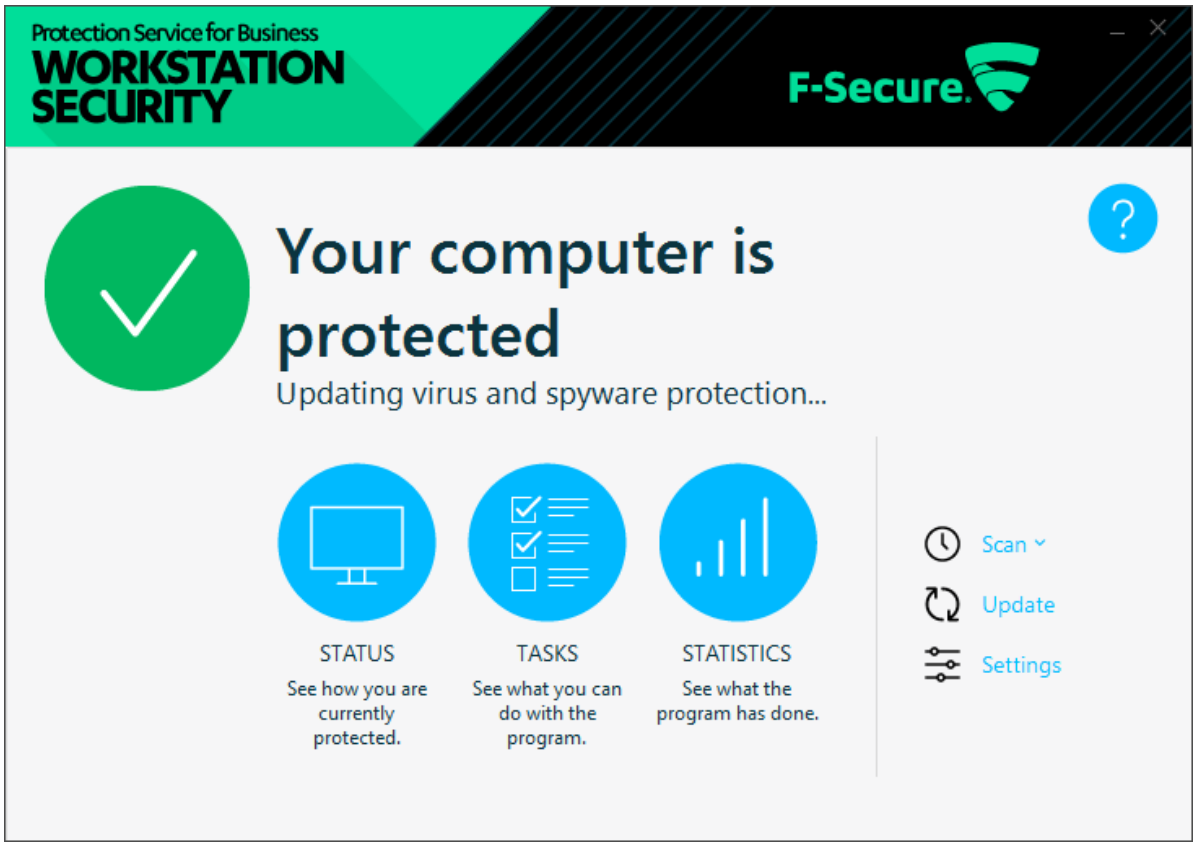
The administrator can run scans and updates, and remove devices from the console, by selecting the checkboxes of the relevant computers on the *Devices* page. A menu panel is then displayed at the bottom of the page, with various relevant commands:

Controlling user access to the endpoint protection software

By default, all users have full control over the client software. Despite creating and applying a policy with the *Allow users to unload products* function disabled, we were not able to change this in our test.

Windows client endpoint protection software

There is a full GUI, similar to a consumer antivirus program:



Tasks available to users

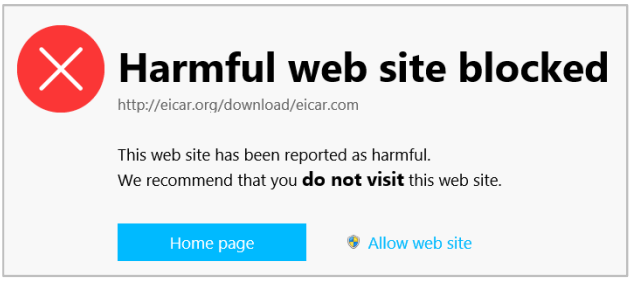
By default, users can access the full range of functionality and settings in the program.

Windows Security Center/Windows Defender

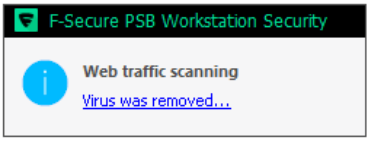
F-Secure Workstation Security registers in Windows Security Center as antivirus and firewall. Windows Defender and Windows Firewall are disabled.

Alerts

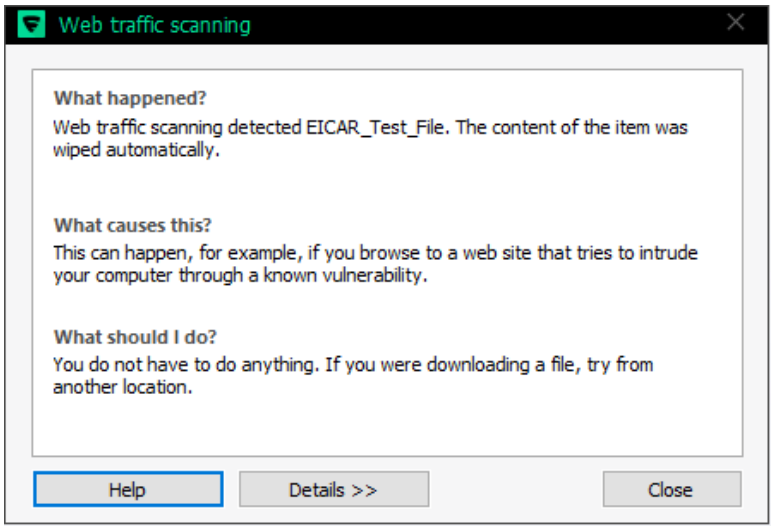
If the EICAR test file is downloaded, the alert below is shown in the browser window:



If the user ignores the warning and clicks *Allow web* site, the file will be intercepted by F-Secure's download protection, which displays a pop-up alert:

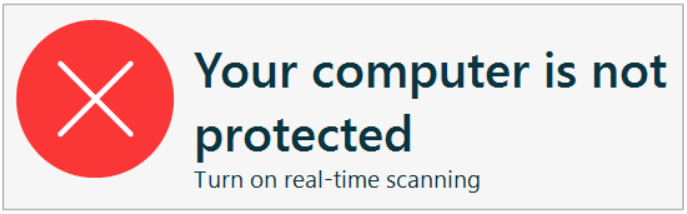


Clicking on this shows a third and final alert:



The user does not need to take any action. The alert persists until *Close* is clicked.

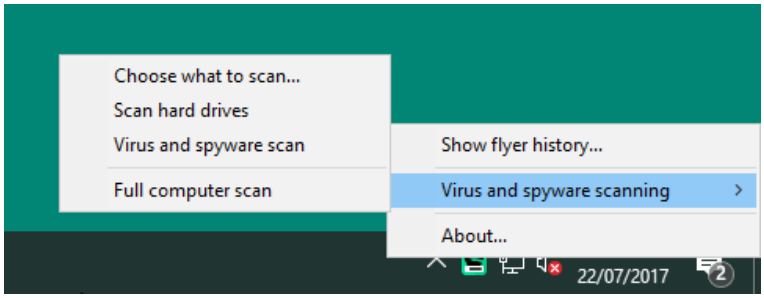
If real-time protection is disabled, the status display in the main program window shows an alert:



The user has to go into the program settings to reactivate the protection.

Windows Server endpoint protection software

The server protection software has a minimalist interface. Right-clicking the System Tray icon displays a context menu which allows the administrator to run malware scans:



G DATA Business Security

Overview

Product version reviewed

G DATA Administrator console 14.0.1.122
G DATA Security Client 14.0.1.122

Windows operating systems supported (for management console and endpoint security)

Clients: XP, Windows Vista, 7, 8/8.1, 10
Servers: Windows Server 2003, 2008/R2, 2012/R2, 2016

About the product

G DATA Business Security uses a server-based console to manage Windows, Mac and Linux clients, Windows Servers and mobile devices.

EDR features

G DATA Business Security does not currently include EDR.

Product information on vendor's website

https://www.gdatasoftware.com/business

Online support

https://www.gdatasoftware.com/support

Summary

G DATA Business Security provides a sophisticated management console that could be used to manage larger networks with multiple servers. It offers a wide range of functions, but its design – similar to the Microsoft Management Console in Windows – will make it familiar and easy to navigate for professional system administrators. The endpoint protection software has a minimalist interface, although admins can allow users to carry out simple everyday tasks such as updates and scans.

Tips for administrators

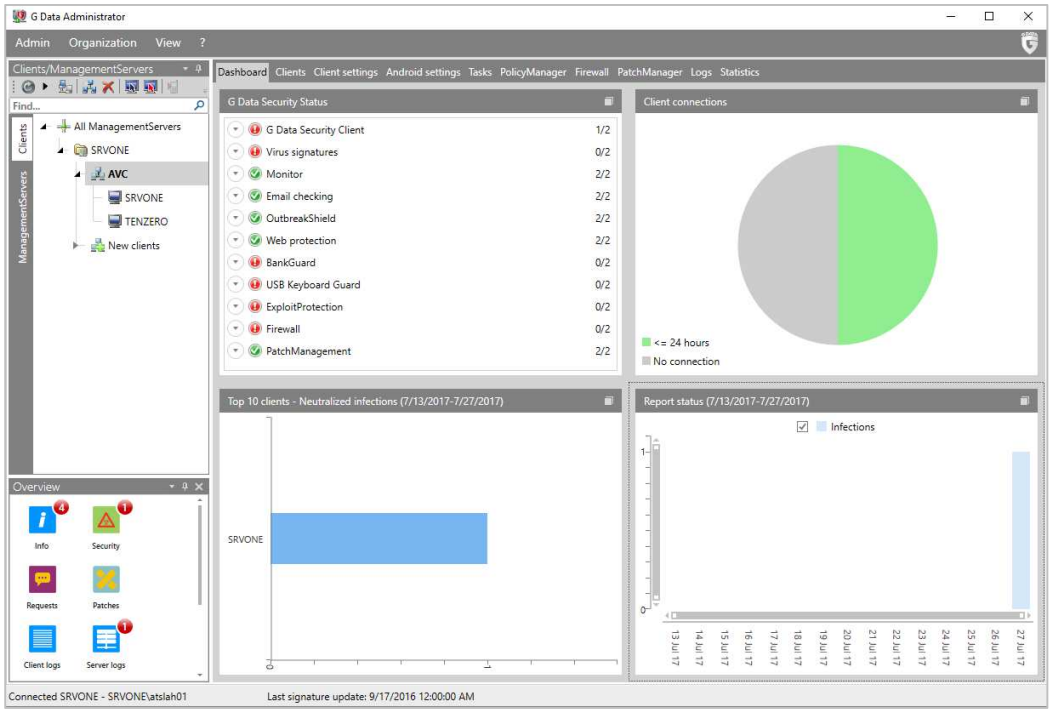
The user manual for the product comes conveniently packaged with the installation files. The section *Installing G DATA Security Client* includes valuable information on preparing client PCs for remote installation (amongst other things).

Management Console

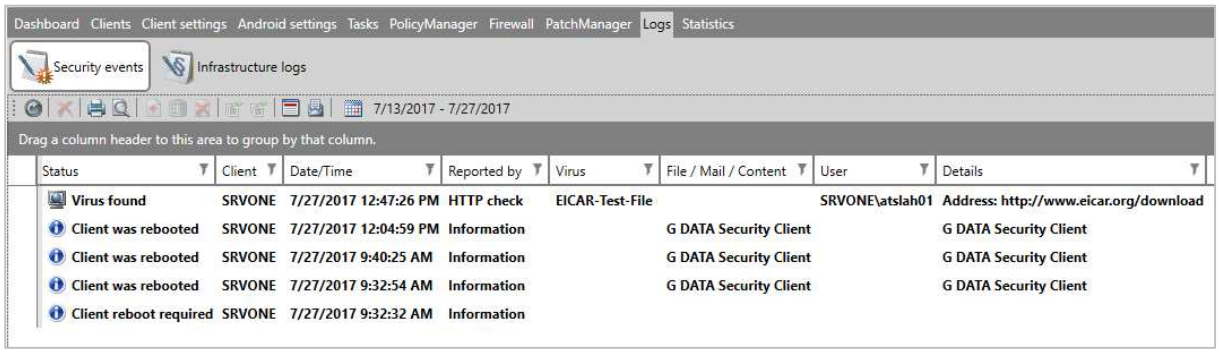
Installation and configuration

The management console is installed on the server by running a single installer file; this includes Microsoft SQL Server 2014 Express, which can be seamlessly installed by the wizard, unless the admin chooses to use an existing SQL Server instance.

Layout



The left-hand menu column allows the admin to select individual computers or computer groups, details of which are shown in the main right-hand pane. The default *Dashboard* view provides an overview of the security status, including details of individual components, and malware detections and scan reports. A row of tabs along the top of the main pane displays other views, including details of clients, client settings (please see screenshot further below), tasks and logs (shown below).



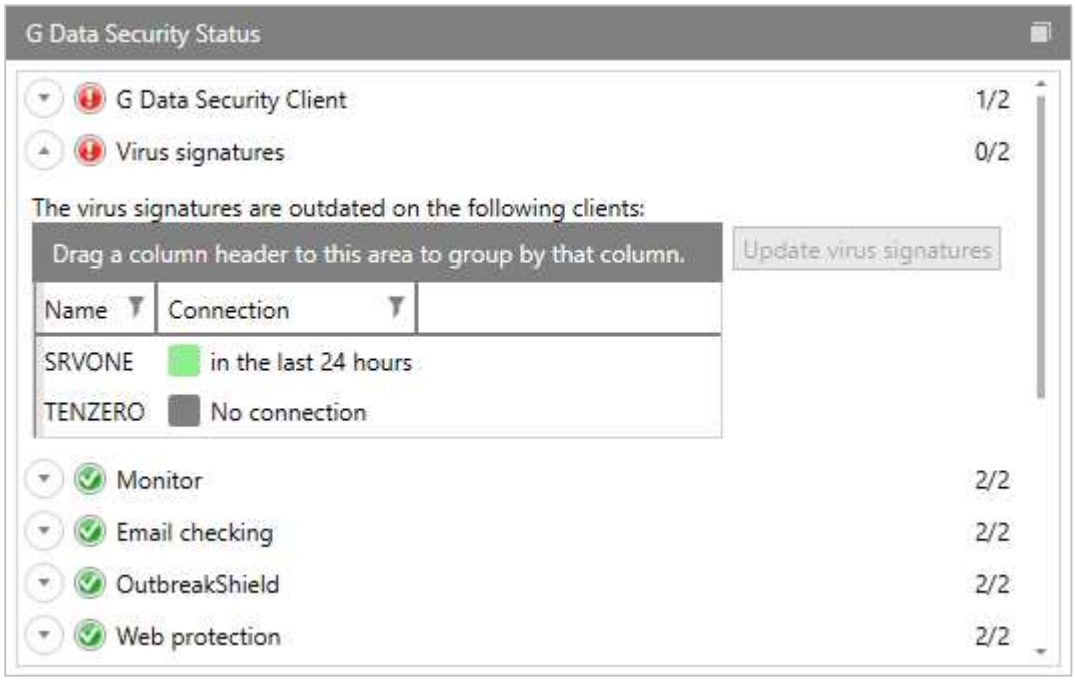
Deployment methods for endpoint protection software

- Remote push installation
- Putting installer file in network share

Monitoring the network

Status and alerts

These are shown in the *G Data Security Status* box in the *Dashboard*. Clicking the arrow symbol to the left of each item displays details of the computers affected:



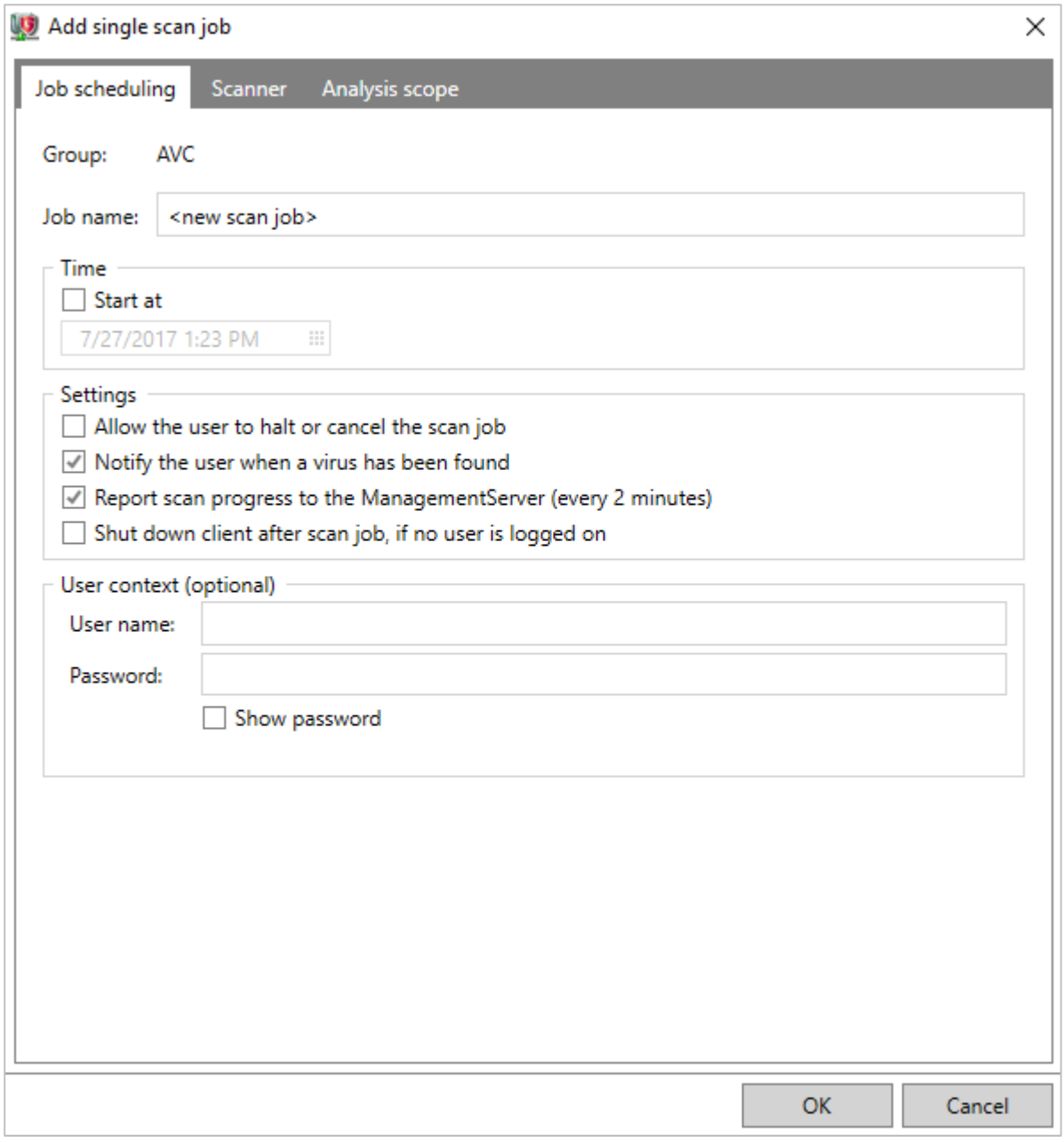
Program version

This is displayed on the *Clients* tab of the main window pane.

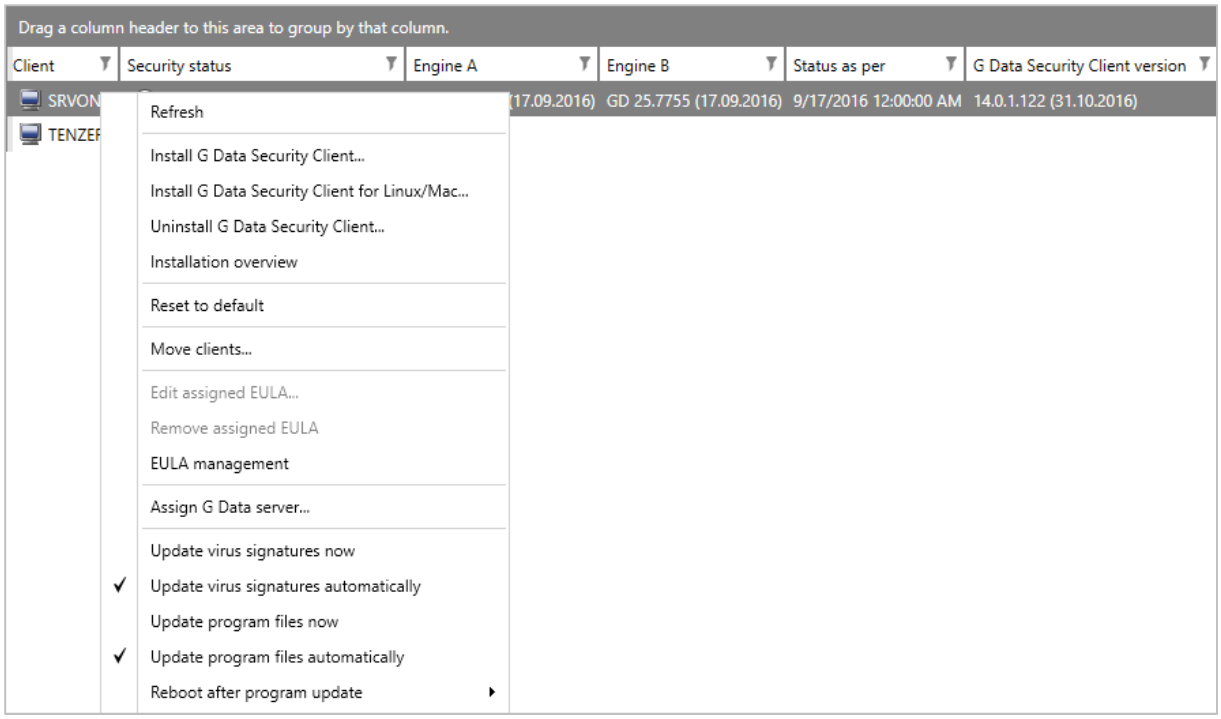
Managing the network

Scanning, scheduling scans, updates and removing devices from the console

One-off and scheduled scans can be run from their respective buttons in the toolbar on the *Tasks* pane. A dialog box provides a number of options:



Client computers can be updated or removed from the console by right-clicking them in the *Clients* tab of the main window pane:



Controlling user access to the endpoint protection software

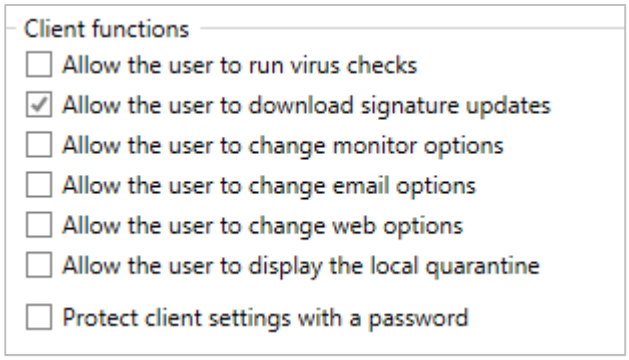
This can be set on the *Client Settings* tab of the main window pane – please see screenshot in the "Tasks available to users" section below.

Windows client endpoint protection software

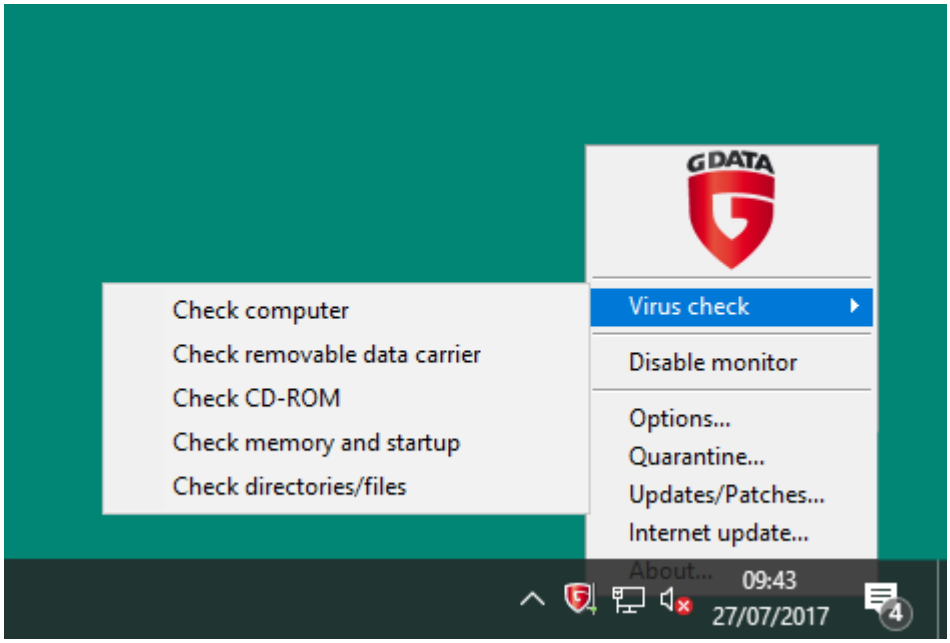
There is a minimal interface, consisting of a System Tray icon, which displays a shortcut menu when right-clicked:

Tasks available to users

By default, the only thing users can do is run a signature update. However, the admin can make additional tasks available from the *Client Settings* page in the console:



This then extends the shortcut menu with the items shown below:



Windows Security Center/Windows Defender

G DATA Security Client registers as the antivirus program in Windows Security Center. Windows Defender is disabled.

Alerts

If the EICAR test file is downloaded, the alert below is shown in the browser window:

No user action is required.

If real-time protection is disabled, a small warning triangle appears over the System Tray icon, and the shortcut menu displays the item *Enable monitor*, clicking which reactivates the protection.

Windows Server endpoint protection software

This can be regarded as being identical to the client protection software.

Kaspersky Endpoint Security for Business Advanced

Overview

Product version reviewed

Kaspersky Security Center 10.4.343
Kaspersky Endpoint Security 10.3.0.6294 AES256

Windows operating systems supported

Endpoint protection software and management console
Clients: Pro and Enterprise editions of Windows 7, 8, 8.1, 10 (32- and 64-bit)
Servers: Windows Server 2008 (32- and 64-bit), 2008 R2, 2012, 2012 R2, 2016

About the product

Kaspersky Endpoint Security for Business Advanced uses a server-based console to manage software for devices with Windows, Mac, Linux, Android, iOS and Windows Phone operating systems.

EDR features

With regard to EDR features, Kaspersky Lab tell us that "*KES becomes available by the end of the year as an integral part of combined Kaspersky Endpoint Detection and Response solution to protect against targeted attacks, as well as a standalone Kaspersky Endpoint Security 11. Kaspersky EDR provides security teams and Security Operations Centers with: enhanced incident mitigation, better visibility over endpoints, endpoint protection and investigative capabilities. The customers benefit from Kaspersky Lab's experience in threat intelligence, advanced protection technologies and a long history of discovering the world's most high-profile APTs, all embedded into the solution's threat hunting functionality.*"

Product information on vendor's website

https://www.kaspersky.com/small-to-medium-business-security/endpoint-advanced

Online support

http://support.kaspersky.com/#s_tab4

Summary

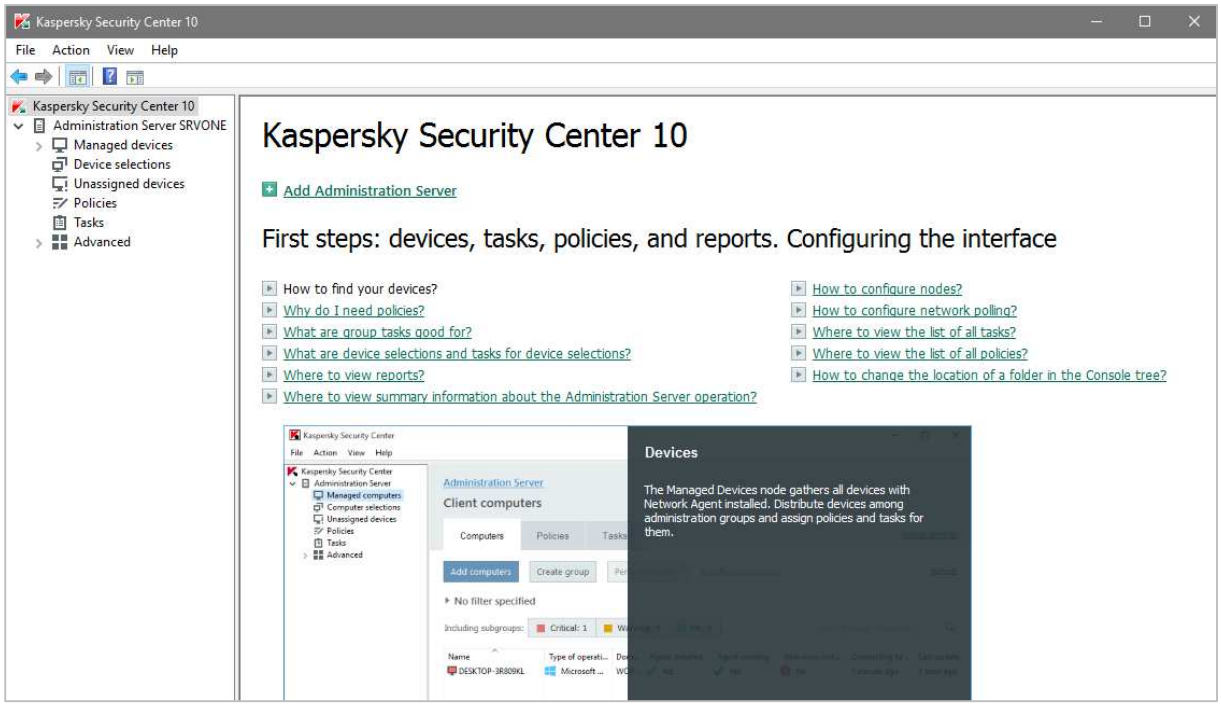
Kaspersky Endpoint Security for Business Advanced allows a very comprehensive range of devices to be supported. The design of the MMC-based console will prove very familiar and easy to navigate for Windows administrators. We particularly liked the opening page, *Kaspersky Security Center 10*, which is essentially an illustrated FAQ page (please see screenshot further below). Consideration has been shown for less-experienced administrators new to AV management consoles, by explaining things such as policies and group tasks.

Management Console

Installation and configuration

The installer file runs a fairly standard Windows installation wizard. This points out that .NET Framework 3.5 is required; the admin can install pause the wizard, install the component, and continue with the installation afterwards.

Layout



Kaspersky Security Center uses the Microsoft Management Console framework, with the left-hand pane used to show the menu items *Managed devices*, *Device selections* (used to group together devices in order to perform a particular action such as updating), *Unmanaged devices, Policies, Tasks* and *Advanced* (various items including *Remote Installation* and *Mobile Device Management*).

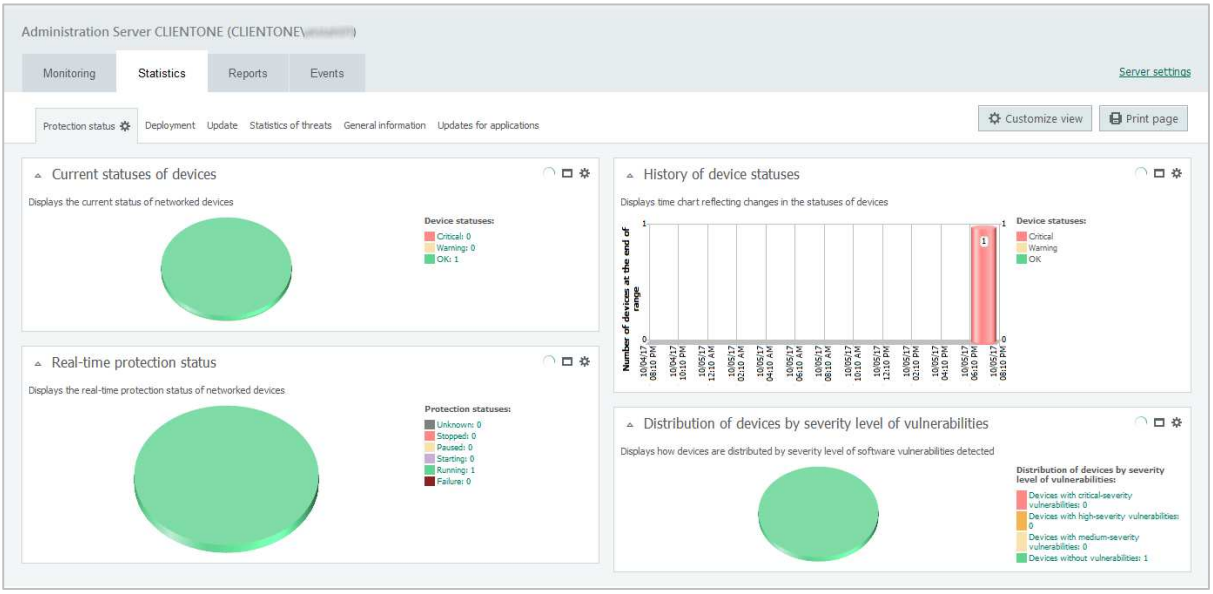
Deployment methods for endpoint protection software

- Distributing installer file by network share/removable device
- Remote push installation

Monitoring the network

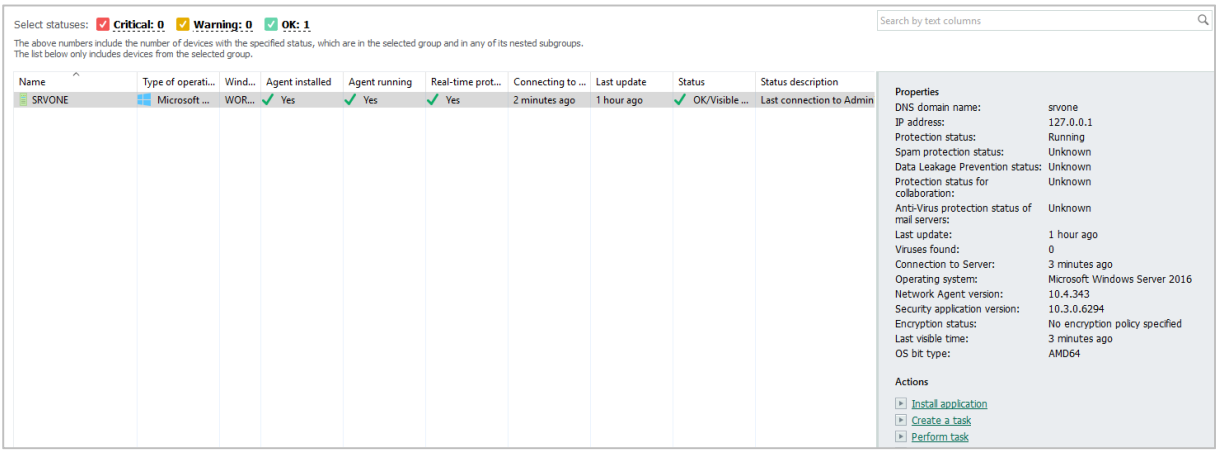
Status and alerts

These are most easily viewed by clicking on the management server in the left-hand pane of the console, then *Statistics, Protection status*. This displays the overall security status, real-time protection status and devices with vulnerabilities in the form of pie charts:



Program version

This can be seen in the properties pane of a device on the *Managed devices* page:



Managing the network

Scanning, scheduling scans, updates and removing devices from the console

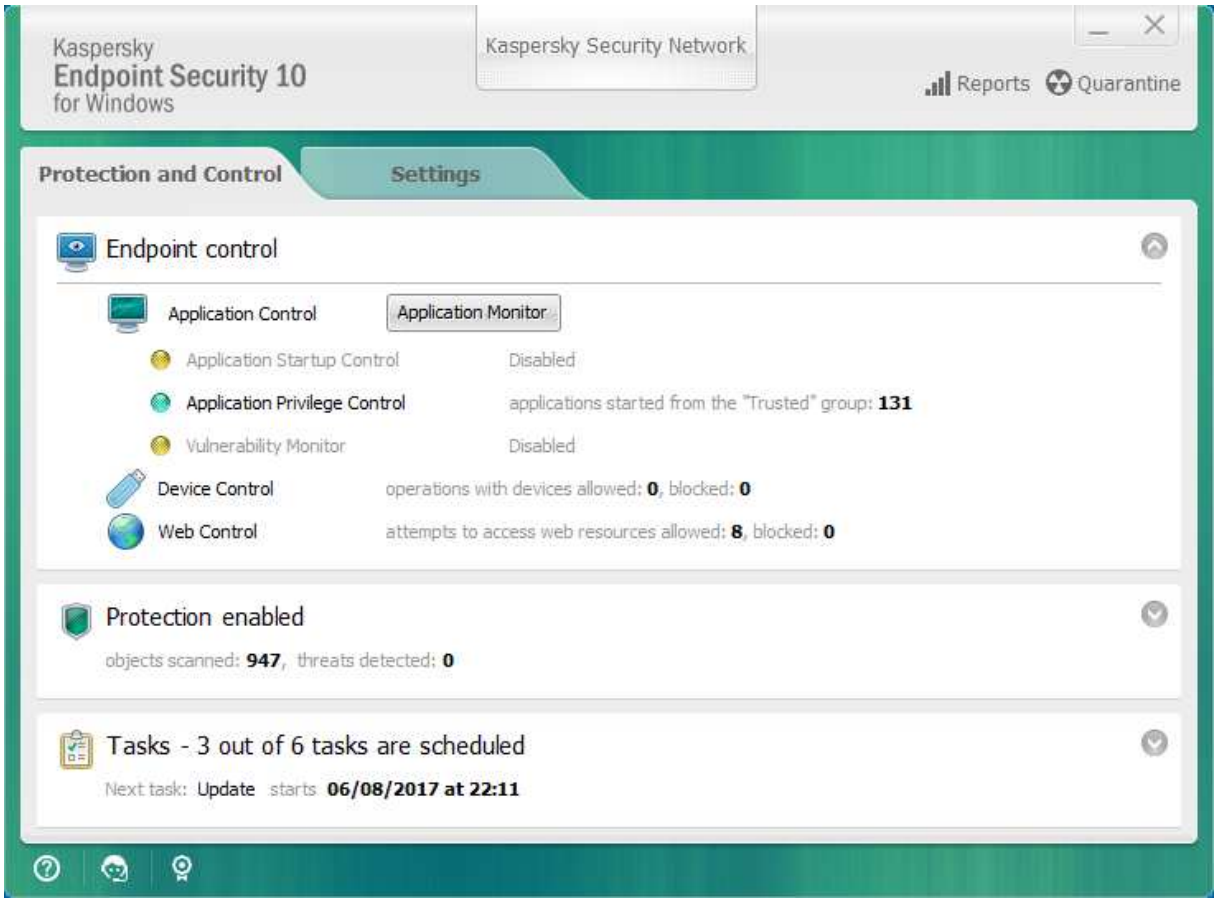
Updates and scans, including scheduled scans, can be run by selecting devices on the *Managed devices* page and clicking *Perform action, Create a task* and running the task wizard.

Controlling user access to the endpoint protection software

By default, all users are able to disable the endpoint protection software. However, this can be prevented by creating and applying a policy with password protection.

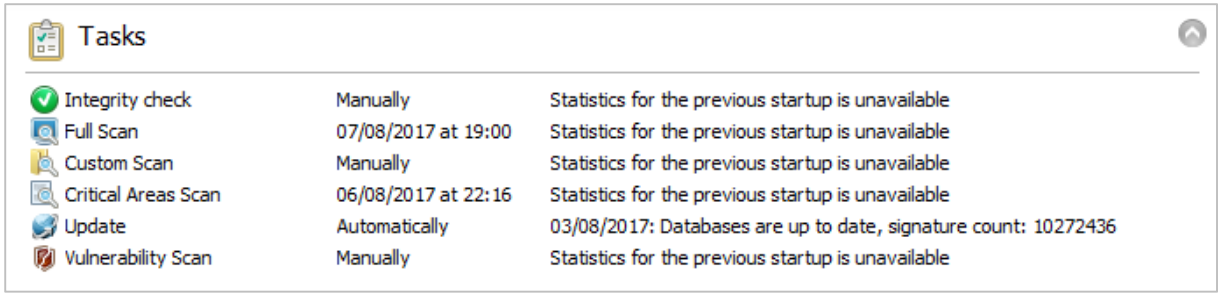
Windows client endpoint protection software

There is a full GUI, although this differs somewhat from a consumer antivirus program, with the emphasis on a detailed status display:



Tasks available to users

Users can run updates and a variety of scans from the *Tasks* section at the bottom of the program window:



Windows Security Center/Windows Defender

Kaspersky Endpoint Security registers as the antivirus and firewall programs in Windows Security Center. Windows Defender and Windows Firewall are disabled.

Alerts

If the EICAR test file is downloaded, the alert below is shown in the browser window:

No user action is required.

If real-time protection is disabled, this is shown in the *Protection* section of the program window, under *File Anti-Virus*. Clicking on this entry displays a menu from which the protection can be reactivated:

Windows Server endpoint protection software

This can be regarded as identical to the client software, except that some components not relevant to a server, such as instant messenger protection, are not installed.

Palo Alto Networks Traps

Overview

Product version reviewed

Palo Alto Networks Traps client software version 4.0.1.25216
Palo Alto Networks Endpoint Security Manager version 4.0.1.25216

Windows operating systems supported

Clients: Windows XP (SP3 and later), Vista (SP1 and later), 7, 8, 8.1, 10
Servers: Windows Server 2003 (SP2 and later), 2008/R2, 2012/R2, 2016

About the product

Palo Alto Networks Traps advanced endpoint protection uses a multi-method prevention approach that secures endpoints against known and unknown malware and exploits and pre-emptively blocks these cyber threats from compromising endpoints.

EDR features

Palo Alto Networks Traps does not contain EDR features as such. However, the vendor states the following: "*Traps currently can collect and display information around all executed process and office documents. This is visible from the Hash Control screen within the Endpoint Security Manager. Traps can also perform queries against the deployed agents. These queries include the ability to look up a registry key, a file or a folder path. Traps, via the WildFire integration, can provides a detailed report for every file executed in the environment. This report includes all information around the behaviours a file exhibited when launched. Lastly, Palo Alto Networks has a separate product that came through the acquisition of the company LightCyber*".[5]

Product information on vendor's website

https://www.paloaltonetworks.com/products/secure-the-endpoint/traps

Online support

https://live.paloaltonetworks.com/t5/custom/page/page-id/Support

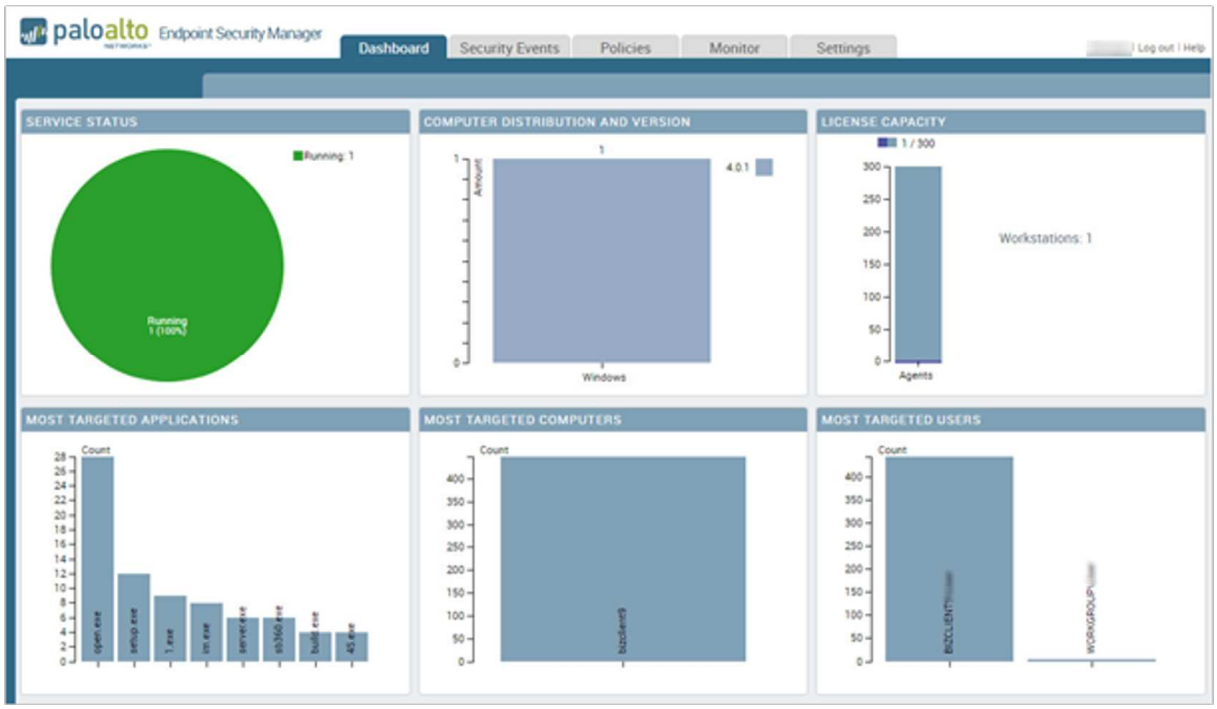
Summary

Whilst the functionality of Palo Alto Networks Traps differs from that of conventional endpoint security products, the Palo Alto Networks Traps Endpoint Security Manager console makes discovering the new features very intuitive. We found the console very well designed and easy to navigate. The product is probably best suited to businesses large enough to have their own IT department.

[5] Palo Alto Networks Completes Acquisition of LightCyber - https://www.paloaltonetworks.com/company/press/2017/palo-alto-networks-completes-acquisition-of-lightcyber
Palo Alto Networks Announces Availability of New Cloud-Based Logging Service - https://www.paloaltonetworks.com/company/press/2017/palo-alto-networks-announces-availability-of-new-cloud-based-logging-service

Management Console

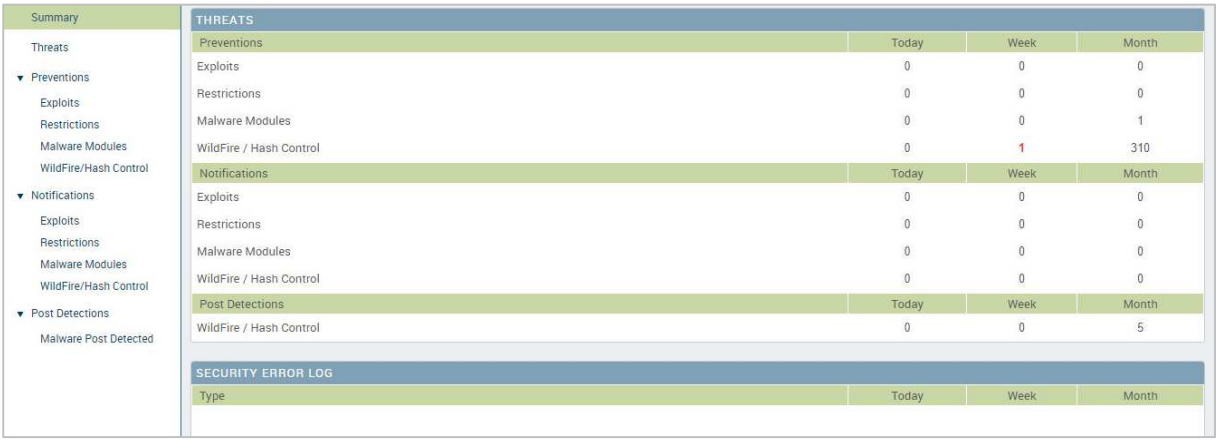
Layout and functionality



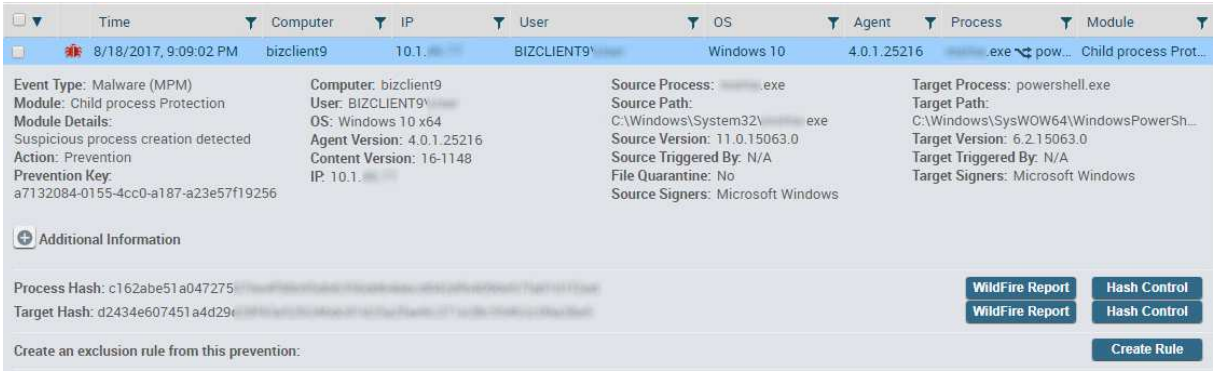
The Endpoint Security Manager console can be navigated using a neat row of tabs at the top of the console (*Dashboard, Security Events*, *Policies*, *Monitor*, and *Settings*).

The console opens on the *Dashboard* page. This provides version and licensing information, as well as the connection status of managed clients. It also provides statistics about which users, computers and applications have been most frequently targeted by threats.

The *Summary* section of the *Security Events* page displays an overview of threats encountered on the network. Threats are organized into groups according to their detection status (*Prevention*, *Notification*, and *Post Detection*) and further divided according to the type of threat encountered.



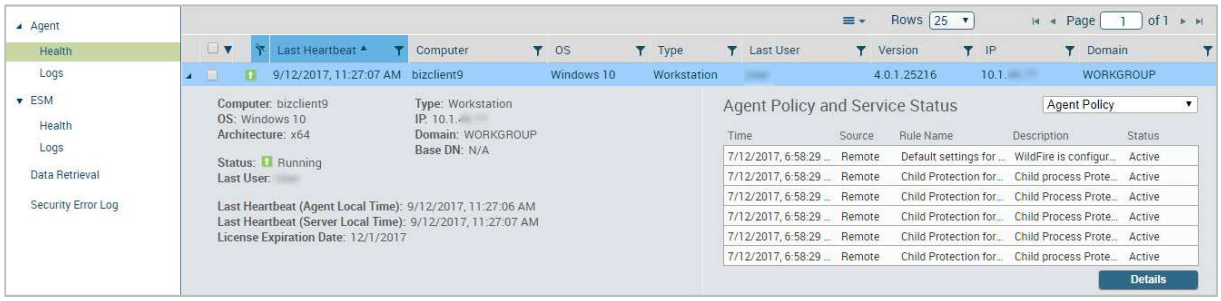
Threat details can be obtained by first selecting the relevant threat category and then selecting the relevant threat from the list displayed:



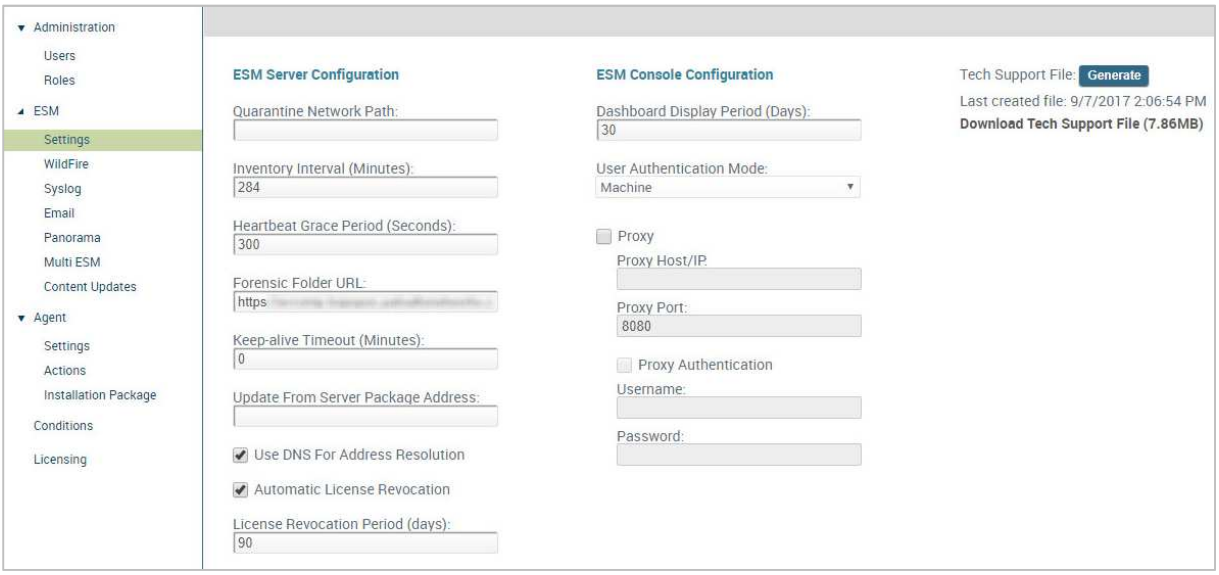
The *Policies* tab allows configuration settings for clients etc. to be modified:

The *Agent Health* section of the *Monitor* page lists clients in the network:

Information about a specific device can be obtained by clicking on its entry:



The *Settings* page allows the console itself to be configured:



Deployment methods for endpoint protection software

- Download and run installer directly
- Share installer via network share or removeable device

Windows client endpoint protection software

The client software has a GUI with a status display, and provides information on malware protection events, running processes and applicable policies:

Tasks available to users

There are no malware-protection tasks that can be carried out by the user, although it is possible to change the interface language under *Settings*.

Windows Security Center/Windows Defender

Palo Alto Networks Traps registers with Windows Security Center as the antivirus program. Windows Defender is disabled.

Administrators have the option of disabling the registration and allowing both Microsoft Windows Defender and Palo Alto Networks Traps to run together on an endpoint.

Alerts

In our test, the EICAR test file was not recognised by Traps, but the AMTSO Potentially Unwanted test file was blocked, and the following alert was shown:

No user action is required. The alert persists until closed by the user.

Windows Server endpoint protection software

This can be regarded as identical to the client software.

Panda Adaptive Defense 360

Overview

Product version reviewed

Panda Adaptive Defense 360 endpoint protection client 7.70.0

Windows operating systems supported

Clients: Windows XP, Vista, 7, 8, 8.1, 10
Servers: Windows Server 2003, 2008/R2, 2012/R2, 2016

About the product

Panda Adaptive Defense 360 uses a cloud-based console to manage security software for Windows clients and servers.

EDR features

With regard to EDR features, Panda state the following: "*The solution classifies all programs and applications running on endpoints through machine learning techniques and the supervision of Panda Security's malware experts. As a result, only those items that are classified as trusted are allowed to run. The endpoint telemetry is the input for the Threat Hunting and Investigation Service (THIS) that searches and notifies customers, when anomalies in applications usage are found. It is also available in real time through applications specifically designed for internal SOCs, MSSPs and MDR providers.*"

Product information on vendor's website

http://www.pandasecurity.com/usa/intelligence-platform/solutions.htm

Online support

http://www.pandasecurity.com/support/adaptive-defense-360.htm

Summary

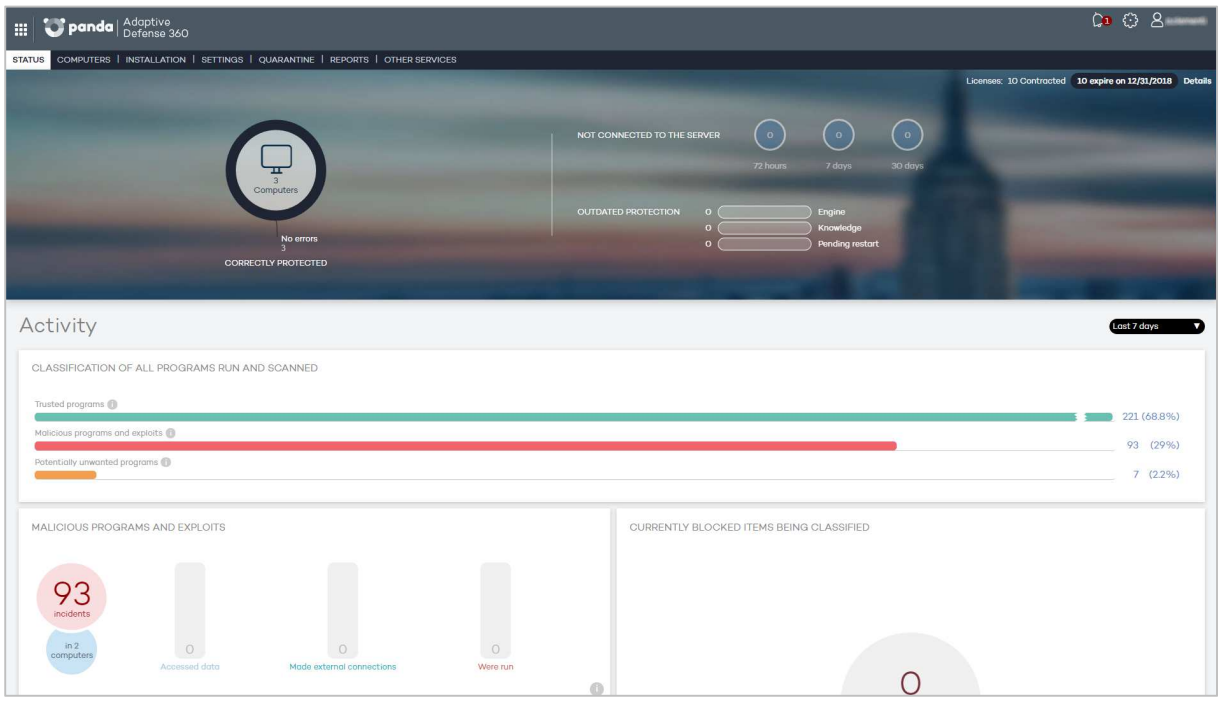
We found Panda Adaptive Defense 360 to be very simple to use. Due to the cloud-based console and easy installation, getting protection up and running is a quick and simple task. The design of the console is very clean and easy to navigate, making it particularly suitable for smaller businesses without permanent IT staff. Bigger companies will appreciate its EDR features too.

Management Console

Installation and configuration

The console is cloud-based, so no setup is required.

Layout



The console opens on the *Status* page. A slim, neat menu bar along the top of the console provides access to the pages *Computers, Installation, Settings, Quarantine, Reports* and *Other Services*.

Deployment methods for endpoint protection software

- Share installer file via network share or removable device
- Access installation URL from browser

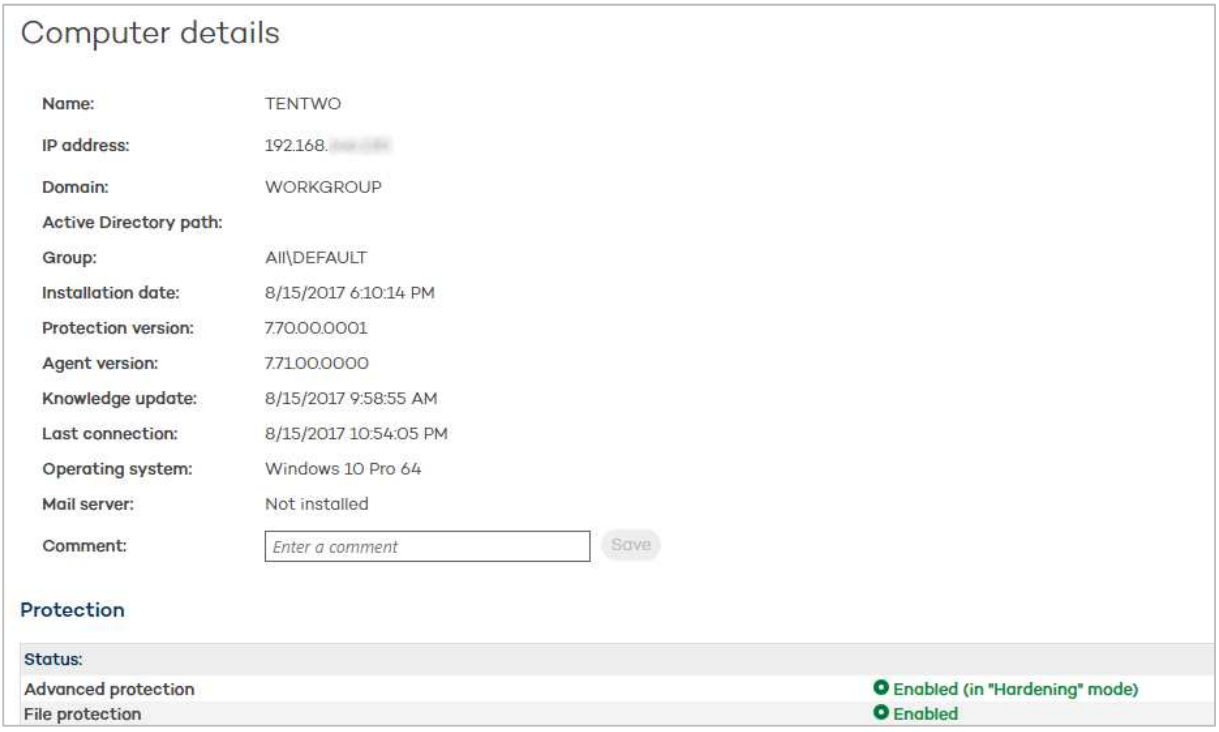
Monitoring the network

Status and alerts

These are shown on the *Status* (home) page of the console. In addition to the basic status information shown at the top of the page (number of computers with any sort of problem), more detailed items are shown below, including *Classification of all programs run and scanned, malicious programs and exploits, currently blocked items being classified, potentially unwanted programs, detection origin* and *web access*.

Program version

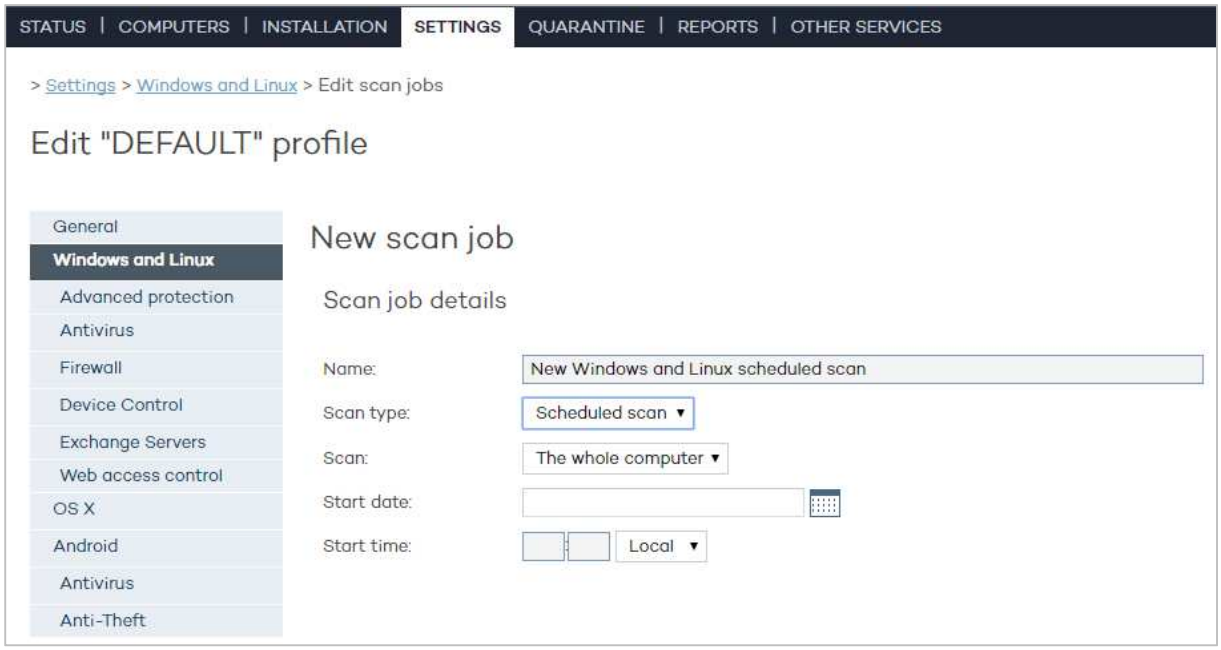
This, along with other key data, is shown on the details page of each client under *Computers*:



Managing the network

Scanning, scheduling scans, updates and removing devices from the console

Scans can be run by clicking *Settings* in the console menu bar, then *Default, Windows and Linux, Scheduled scans, New*. The scan can be run straight away by setting the *Scan type* to *Immediate scan*, or scheduled by selecting *Scheduled scan*:



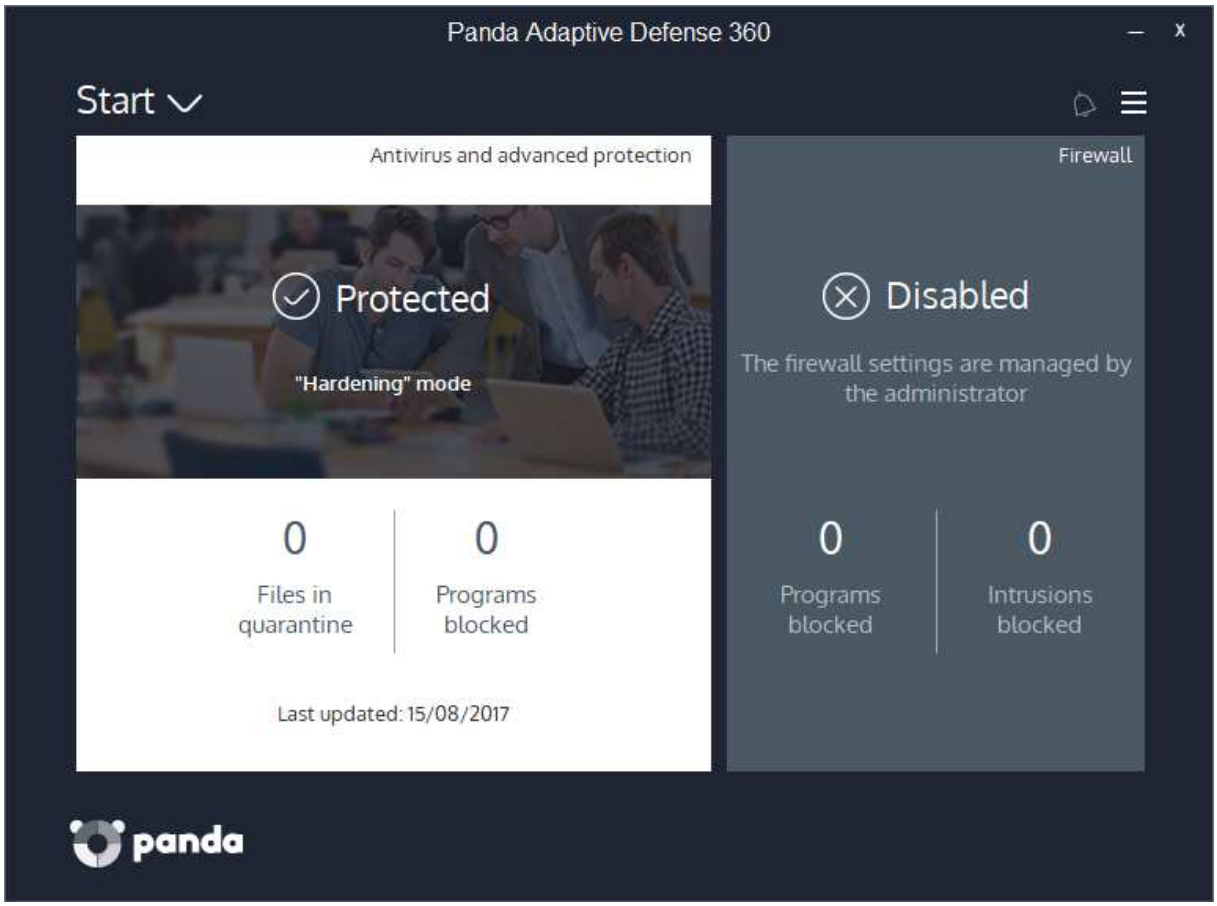
Updates are run on a schedule, details of which can be edited under *Settings\Default\Windows and Linux\Updates*. A computer can be removed from the console by clicking *Computers,* selecting the device in question, and clicking *Delete*.

Controlling user access to the endpoint protection software

The user interface of the client software does not allow users to disable any protection components, this can only be done from the console.

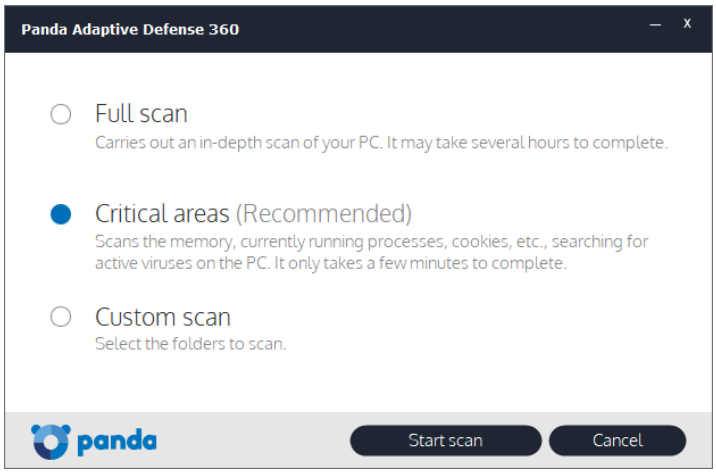
Windows client endpoint protection software

There is a full GUI, similar to a consumer antivirus program:



Tasks available to users

Users can run full, custom or quick (*Critical areas*) scans by clicking *Start, Antivirus and advanced protection, Scan now*:

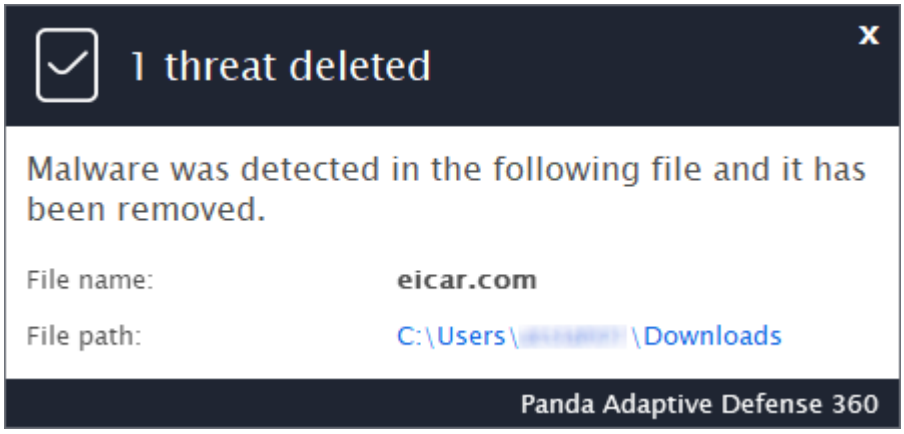


Windows Security Center/Windows Defender

Panda Adaptive Defense 360 registers as the antivirus program in Windows Security Center, and Windows Defender is disabled.

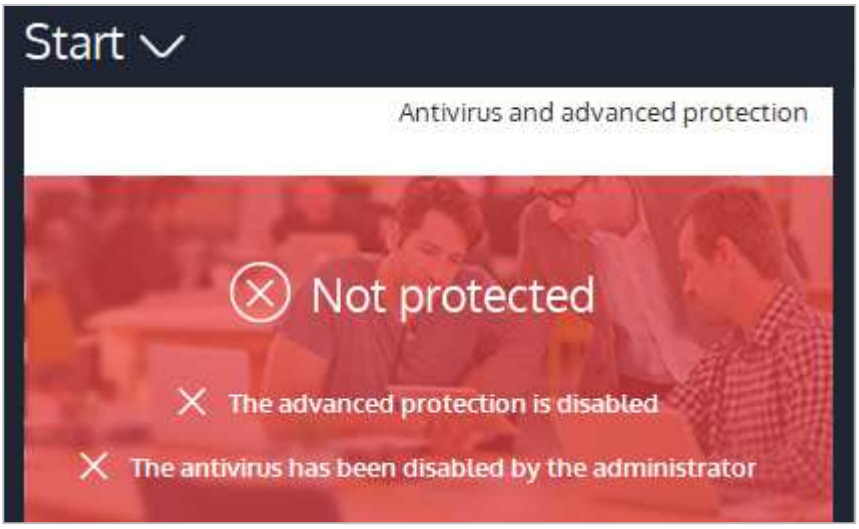
Alerts

If the EICAR test file is downloaded, the alert below is shown:



The user does not need to take any action. The alert closes after a few seconds.

If real-time protection is disabled, a warning is shown in the program window:



The protection has to be reactivated from the console.

Windows Server endpoint protection software

This can be regarded as identical to the client software. However, in our test, we found that Windows Defender in Windows Server 2016 was not disabled by the Panda installer, and continued to run.

SentinelOne Endpoint and Server Protection

Overview

Product version reviewed

SentinelOne Agent 1.8.5.8029

Windows operating systems supported

Clients: Windows XP, 7, 8, 8.1, 10
Servers: Windows Server 2008 R2, 2012/R2, 2016

About the product

SentinelOne uses either a server-based or a cloud-based console to manage Windows, Mac OS and Linux clients, plus Windows and Linux servers.

EDR features

With regard to EDR features, SentinelOne state the following: *"SentinelOne offers several key EDR capabilities: a) detect security incidents at runtime using behavioural AI to monitor processes, files, registries, network etc; b) contain incidents at the endpoint to minimize impact; c) investigate incidents to understand execution characteristics and respond holistically; d) automate remediation and rollback of the endpoint to a pre-infection state to help organizations swiftly recover from any incidents. SentinelOne also enables organizations to drive IOC search and threat hunting, including visibility into encrypted traffic, with the Deep Visibility module. Customers can also augment their security teams with remote monitoring and response services via SentinelOne Vigilance"*.

Product information on vendor's website

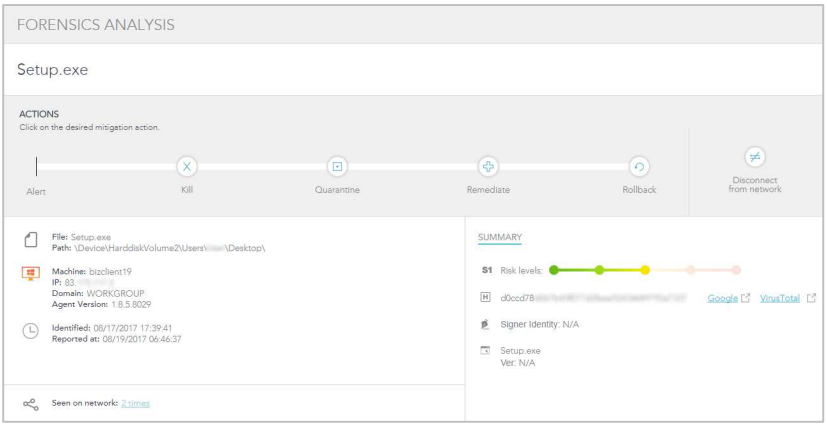
https://sentinelone.com/platform/

Online support

https://sentinelone.com/support/

Summary

Once the admin has grasped the basics of how the protection works, the product is very straightforward to use. Although much detailed information for e.g. threats and actions is provided, the clean, uncluttered and modern layout makes the console very easy to navigate. We particularly liked the information page for each threat, with its convenient links to Google and VirusTotal:

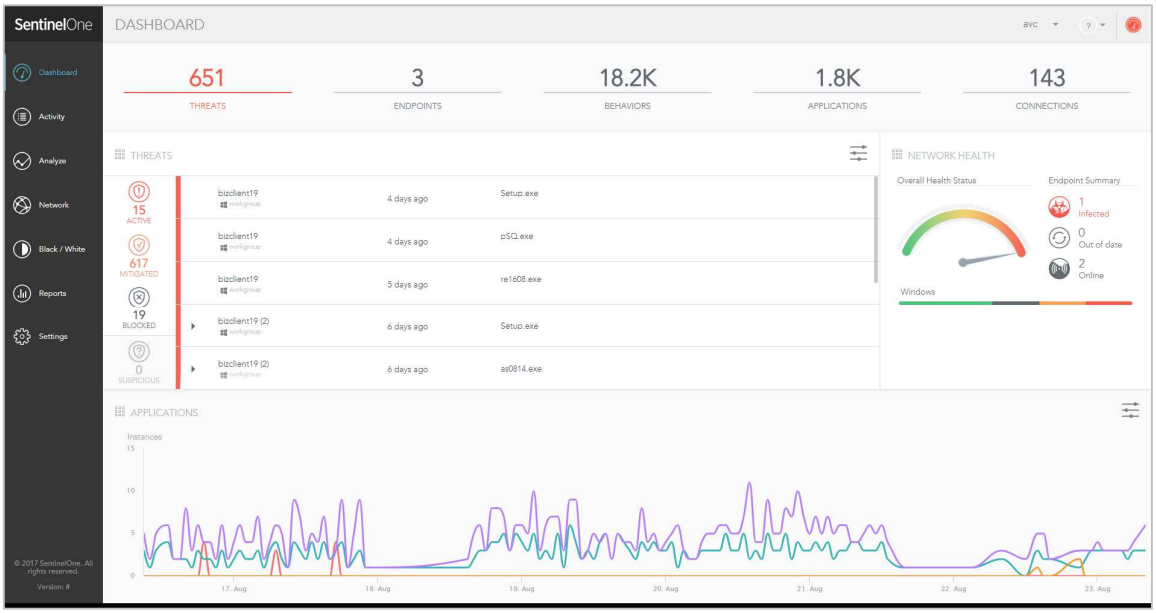


Management Console

Installation and configuration

We tested the cloud-based version of SentinelOne's console, so no installation or configuration was required.

Layout



The console can be navigated using the menu panel on the left-hand side. This provides links to *Dashboard* (system status overview), *Activity* (actions taken by the software), *Analyze* (analysis of suspected malware), *Network* (list of protected devices), *Black/White* (blacklist/whitelist), *Reports,* and *Settings*.

Deployment methods for endpoint protection software

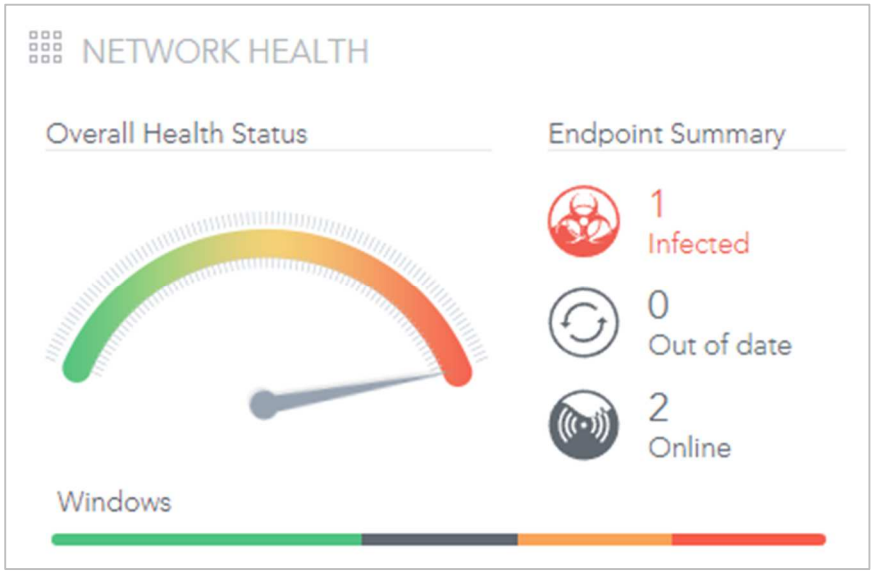
- Download installer from console
- Share installer via LAN or use a third-party deployment tool like SCCM or GPO

Monitoring the network

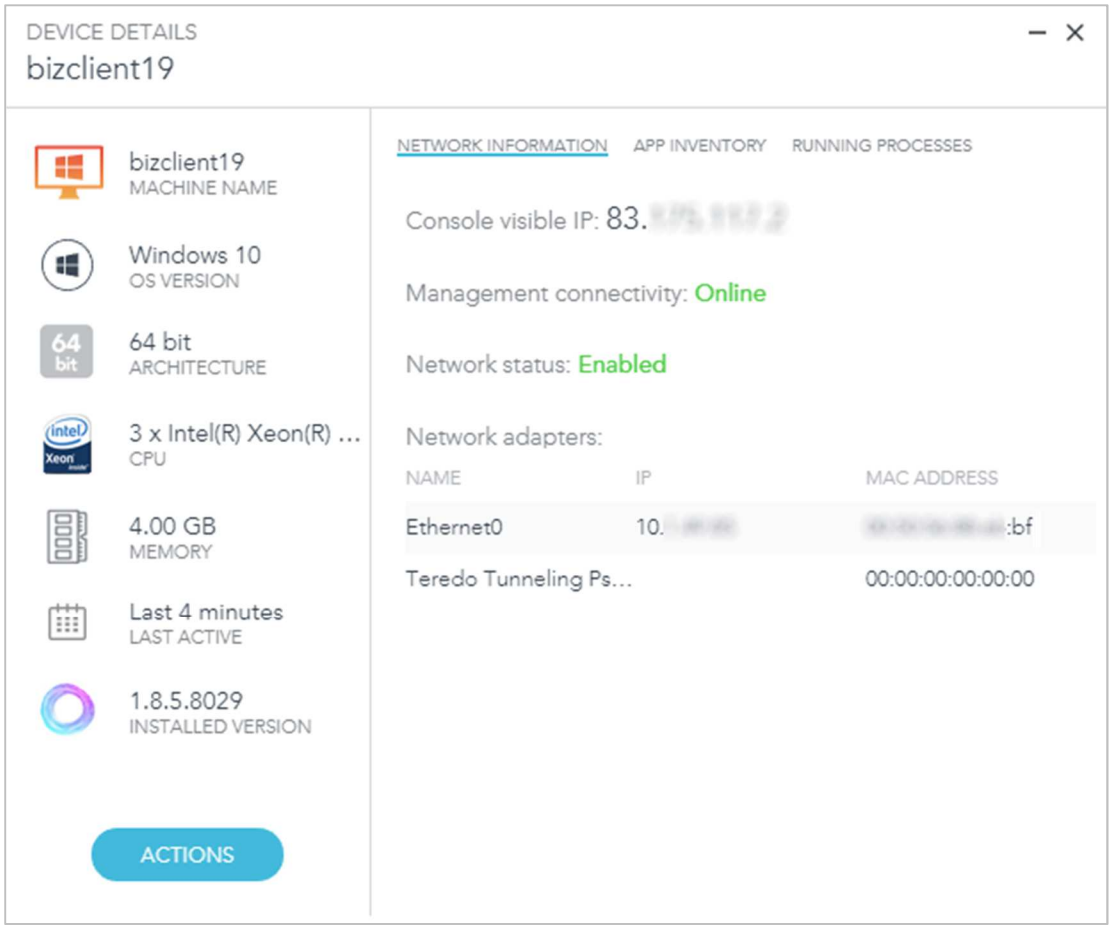
Status and alerts

The *Threats* section on the *Dashboard* page lists all threats monitored on the network. Threats are divided into four categories: *Active*, *Mitigated*, *Blocked*, and *Suspicious*. Threats in the Active category are always displayed first in the threat list. The other categories can be added and removed from the threat list by clicking the respective icon in the management console.

Furthermore, the *Network Health* section on the *Dashboard* page provides a status summary for connected endpoints. The section displays the number of endpoints with detected infections or out-of-date protection software, as well as the number of endpoints currently online.



More detailed information about specific connected endpoints can be retrieved from the *Network* page:



If the endpoint was configured in alert-only mode, an administrator can select a manual mitigation action such as Remediate or Rollback from the More menu and mark the threat as resolved. However, according to the vendor, manual intervention should rarely be needed. Although not set by default, SentinelOne recommends a kill or quarantine mode which automates the mitigation process.

Program version

The version of the installed endpoint protection software can be accessed by opening the details window of the relevant client from the *Network* page or by clicking on any device name from everywhere in the console.

Managing the network

Scanning, scheduling scans, updates and removing devices from the console

Scans can be run by selecting client devices on the *Network* page, then clicking the *Actions* button, *Initiate Scan*. There is a switch for the installer program (*/scheduleFullScan*) that runs a full scan after installation. The scan is being done by its Deep File Inspection feature. Updates to endpoint software or the management console can be performed in the *Updates* section of the *Settings* page.

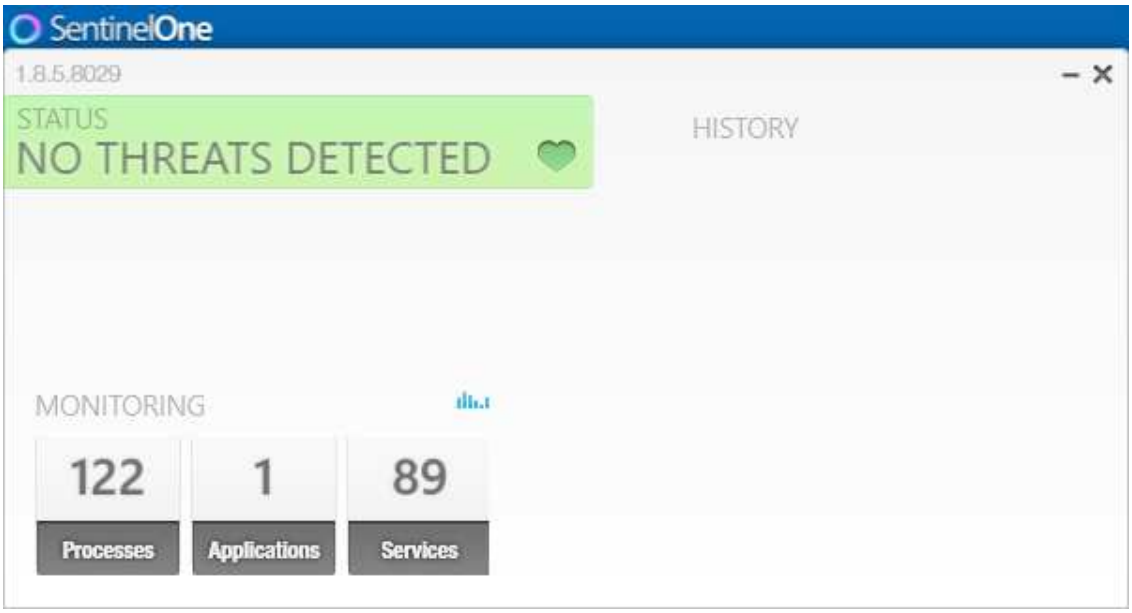
Using the *Actions* menu on the *Network* page, an administrator can uninstall the endpoint software of connected clients, thereby removing those devices from the console.

Controlling user access to the endpoint protection software

There is no means of disabling or reconfiguring the software from the client GUI.

Windows client endpoint protection software

There is a minimal GUI, which shows status and some log items:



Tasks available to users

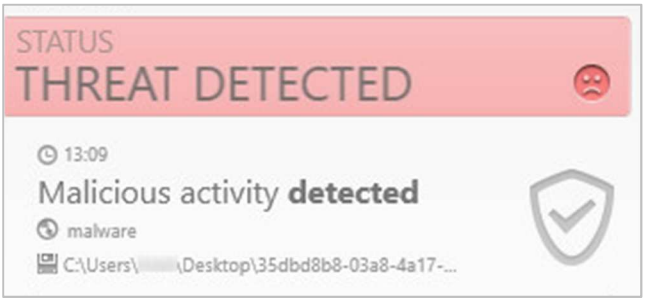
There are no tasks available to users from the GUI.

Windows Security Center/Windows Defender

The Sentinel Agent registers as virus protection in Windows Security Center. Windows Defender is disabled.

Alerts

If the EICAR test file is downloaded, it is blocked silently, i.e. there is no pop-up warning. However, the last item blocked is shown in the main program window:



No user action is required.

Windows Server endpoint protection software

This can be regarded as identical to the client software. However, we found that in our test, Windows Defender on Windows Server 2016 was not disabled by the SentinelOne Agent installation.

Trend Micro OfficeScan

Overview

Product version reviewed

Trend Micro OfficeScan Agent for Windows clients and servers 12.0.1315
Trend Micro OfficeScan Server XG Build 1315

Windows operating systems supported

Management Console
Windows Server 2008/R2, 2012/R2, 2016

Endpoint Protection Software
Clients: Windows XP, 7, 8/8.1, 10, all 32- and 64-bit
Servers: Windows Server 2003/R2, 2008/R2, 2012/R2, 2016

About the product

Trend Micro OfficeScan uses a server-based console to manage Windows clients and servers.

EDR features

Trend Micro OfficeScan does not include the full discovery and investigation features often associated with EDR products, although these are included in another product, Trend Micro Endpoint Sensor[6] which can be centrally managed with OfficeScan via the Trend Micro Control Manager. Endpoint Sensor is an investigation tool designed to speed the discovery, investigation and response to security incidents.

Product information on vendor's website

https://www.trendmicro.com/en_us/business/products/user-protection/sps/endpoint/officescan.html

Online support

https://success.trendmicro.com/product-support/officescan-xg

Summary

Trend Micro OfficeScan provides a sophisticated management console that could be used to manage larger corporate networks, but which nonetheless provides a straightforward interface that makes essential tasks and information easy to access. In our test, we found the process of installing the console and deploying client software to be very efficient and unproblematic, and we were impressed with the speed at which client computers reacted to commands from the console.

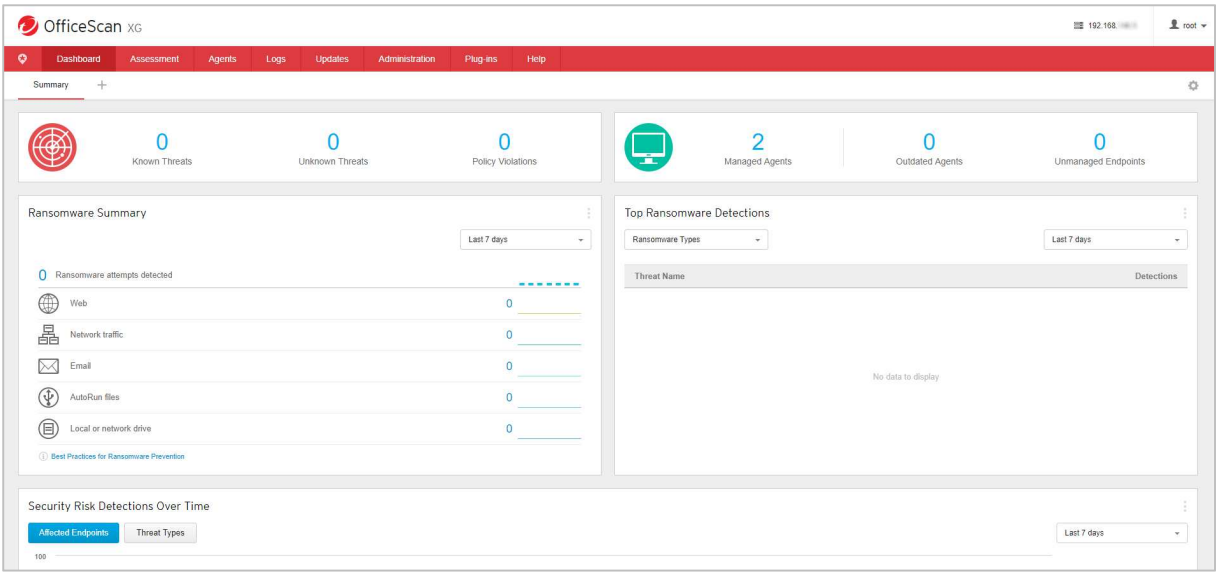
[6] https://www.trendmicro.com/en_us/business/products/network/deep-discovery/endpoint-sensor.html

Management Console

Installation and configuration

To install the management console server on the server, the admin runs the installer file and completes a straightforward setup wizard.

Layout



The console can be navigated by a row of drop-down menus along the top of the console.

Deployment methods for endpoint protection software

- Remote push installation
- Deployment via Active Directory
- Deployment via login script
- Local installation from network share

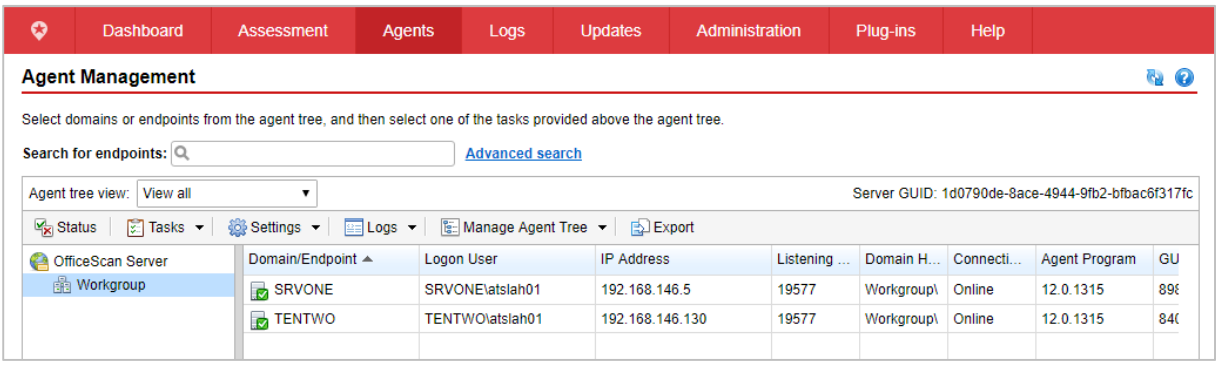
Monitoring the network

Status and alerts

These are shown on the *Dashboard* (home page of the console. Items shown include the status of managed computers, threats discovered, and details of ransomware detections.

Program version

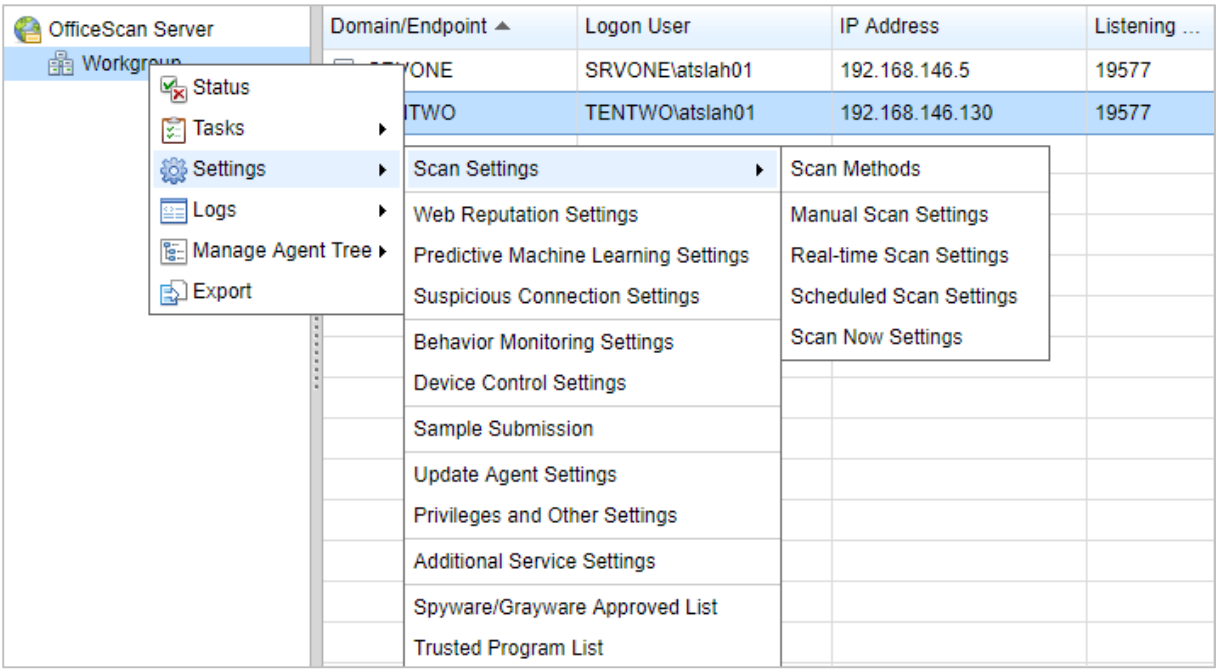
This can be seen by clicking on *Agents, Agent Management* and the workgroup/domain name under *OfficeScan Server*. A wide variety of information is shown for each client, and the order of the columns can be rearranged by drag and drop.



Managing the network

Scanning, scheduling scans, updates and removing devices from the console

Scans can be run by selecting a computer or group on the *Agent Management* page, and clicking *Tasks, Scan Now*. The admin can leave scan settings at their defaults, or change them before starting the scan. Scheduled scans, along with a wide range of other tasks, can be run by right-clicking the computer/group on the same page, and selecting the task required from the appropriate sub-menu:

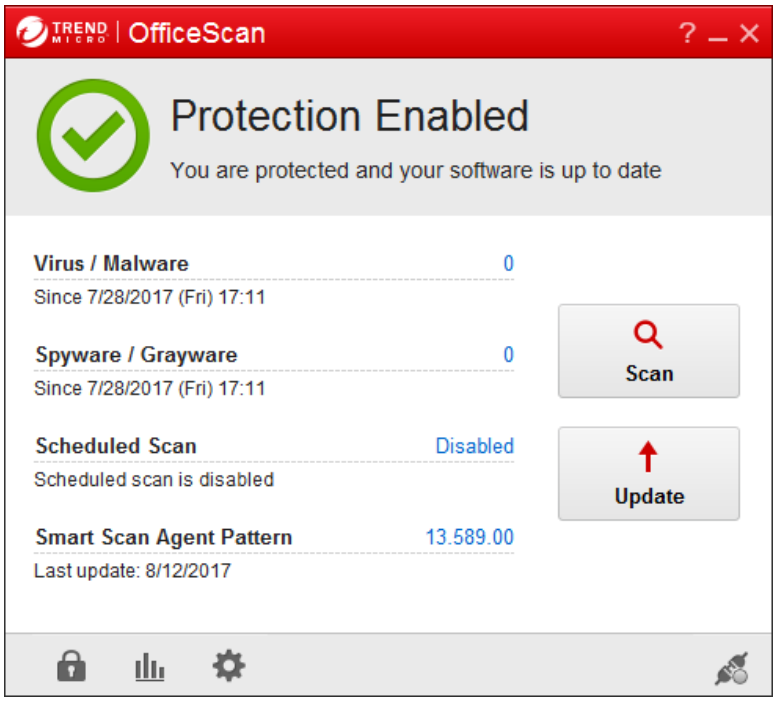


Controlling user access to the endpoint protection software

By default, users cannot change protection settings without entering the password for the administration console.

Windows client endpoint protection software

There is a full GUI, similar to a consumer antivirus program:



Tasks available to users

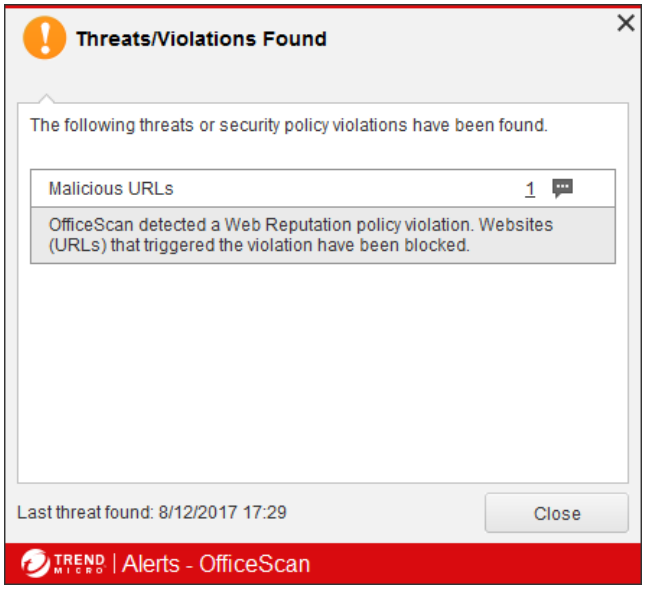
Users can run updates and scans from the user interface.

Windows Security Center/Windows Defender

Trend Micro OfficeScan registers with Windows Security Center as the antivirus and firewall programs. Windows Defender is disabled, but Windows Firewall is not.

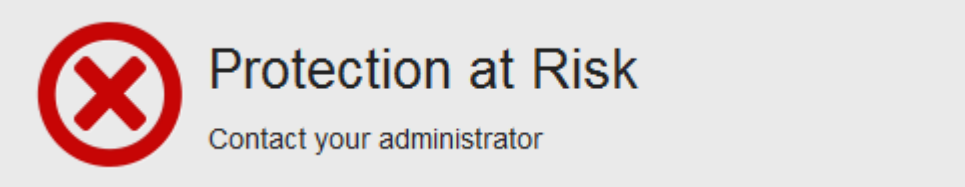
Alerts

If the EICAR test file is downloaded, the alert below is shown:



The alert persists until the user closes it. No user action is necessary.

If real-time protection is disabled, an alert is shown in the status section of the program window:



Protection can only be enabled/disabled from the console.

Windows Server endpoint protection software

This can be regarded as identical to the client software, although by default the Trend Micro Firewall is not installed.

VIPRE Endpoint Security Cloud

Overview

Product version reviewed

VIPRE Business Agent for Windows servers and workstations 10.0.7110

Windows operating systems supported

Clients: Windows Vista, 7, 8.1, 10
Servers: Windows Server 2008/R2, 2012/R2, 2016; Windows Small Business Server 2003, 2008, 2011

About the product

VIPRE Endpoint Security Cloud uses a cloud-based console to manage endpoint protection software for Windows clients and servers.

EDR features

VIPRE Cloud does not currently include any EDR features.

Product information on vendor's website

https://www.vipre.com/products/business-protection/cloud/

Online support

https://www.vipre.com/support/business/

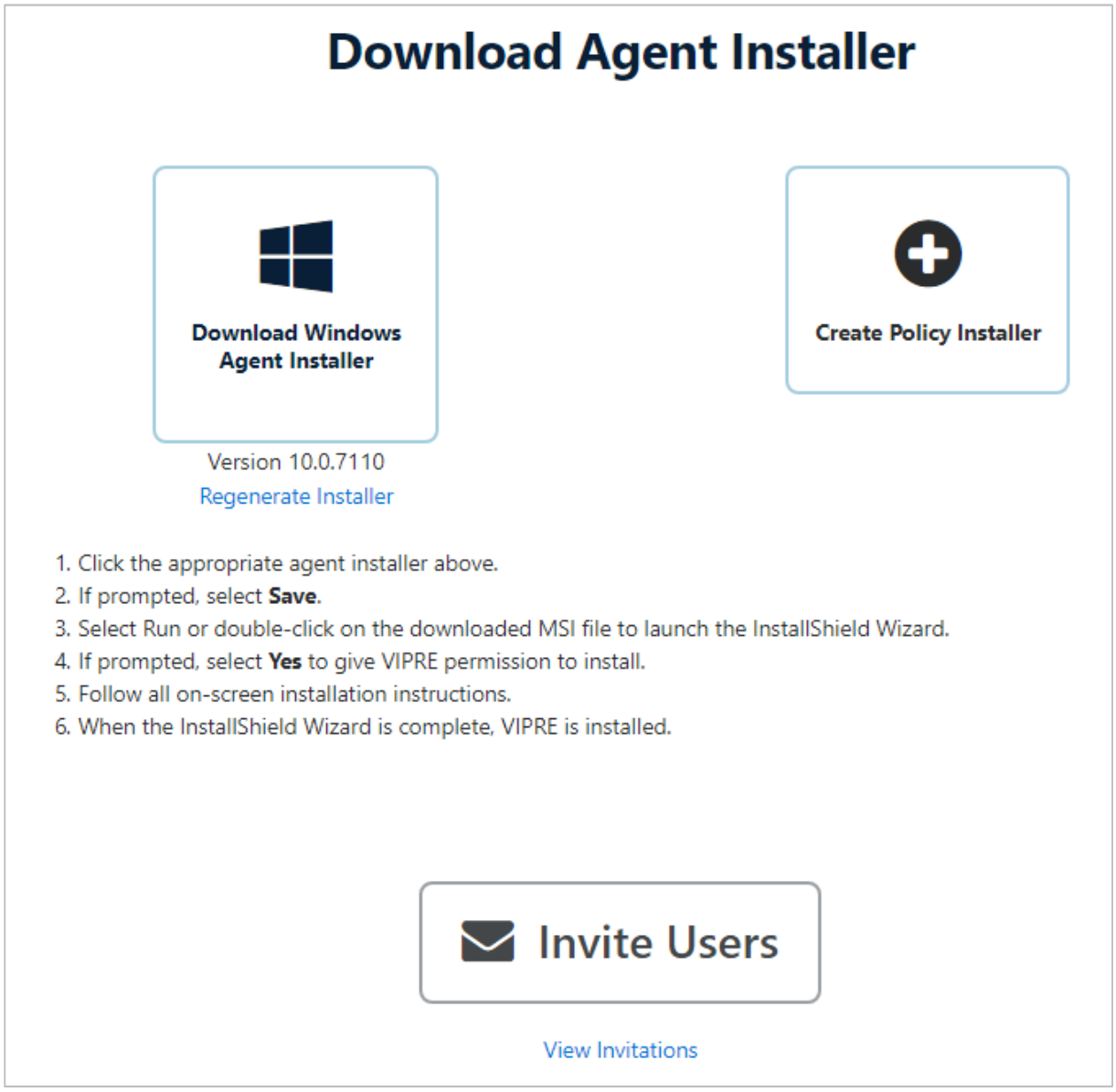
Summary

VIPRE Endpoint Security Cloud provides a very simple, easy-to-use console that makes deployment and everyday management of endpoint security software quick and straightforward. Even less-experienced administrators will find both the management console and the endpoint software very clear and intuitive, making the product an ideal choice for smaller businesses without full-time IT support.

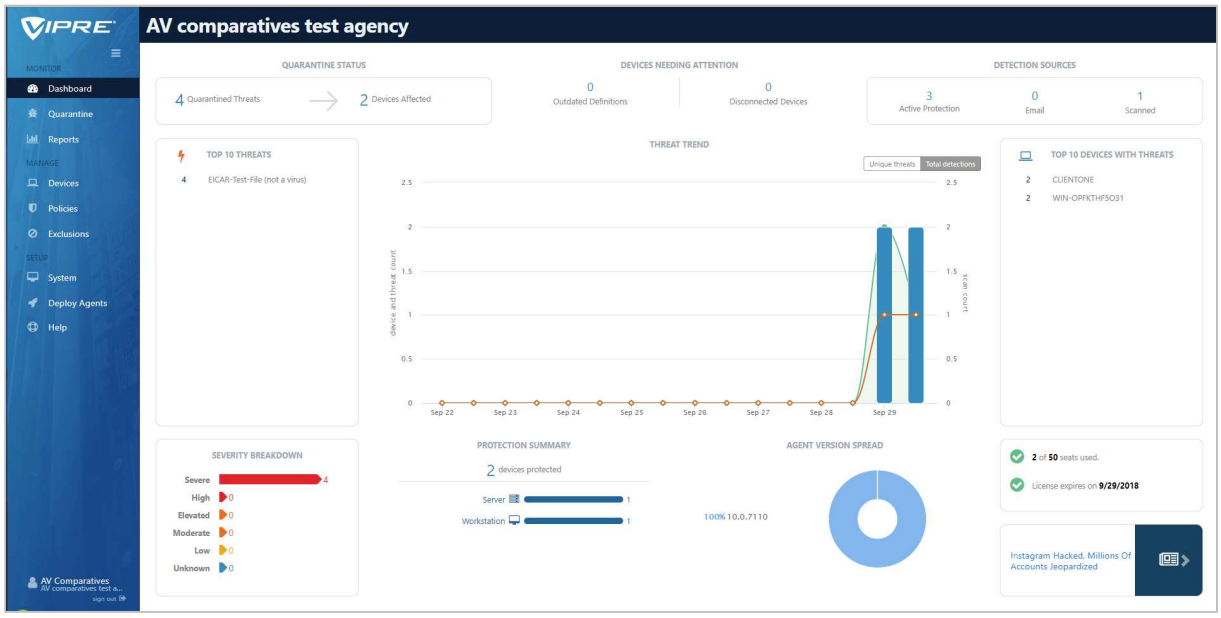
Management Console

Installation and configuration

The console is cloud-based, so no installation or configuration is required. When the admin first logs on to the console, the *Deploy Agents* page is displayed, making it easy to start deployment:



Layout



The console can be navigated from a left-hand menu column, with links to the pages *Dashboard, Quarantine, Reports, Devices, Policies, Exclusions, System, Deploy Agents*, and *Help*. The menu panel can be collapsed to show just the icons, or expanded to include text.

Deployment methods for endpoint protection software

- Download and run installer from console
- Email installation link to users

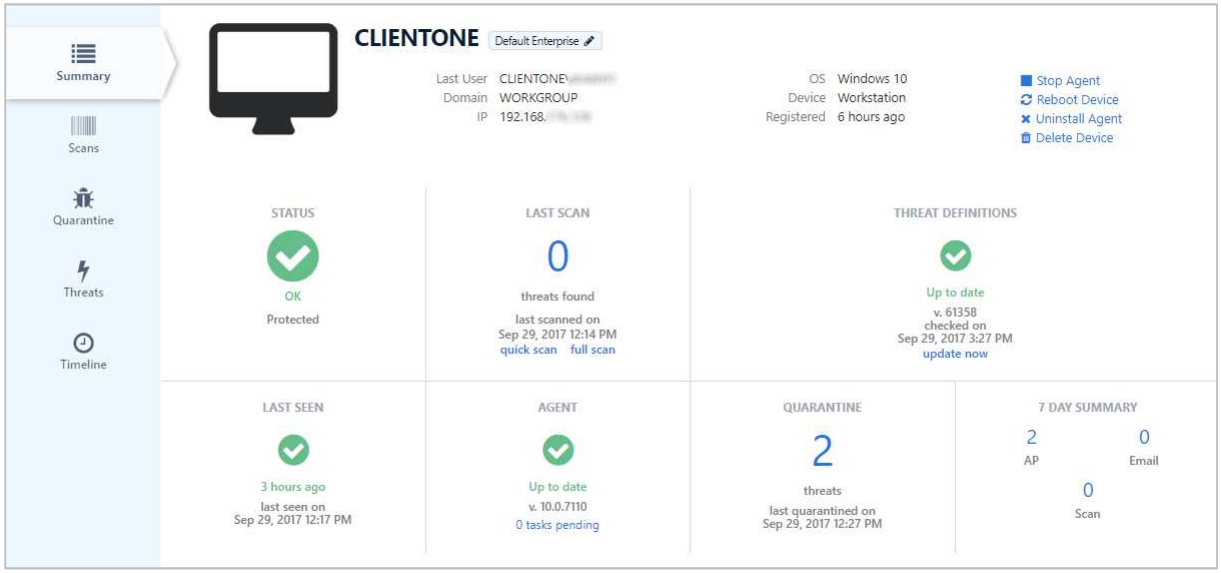
Monitoring the network

Status and alerts

These are shown on the *Dashboard* (home) page of the console. Various panels show *Quarantine, Devices Needing Attention, Detection Sources, Top 10 Threats, Top 10 Devices with Threats, Severity Breakdown, Protection Summary,* and *Agent Version Spread.*

Program version

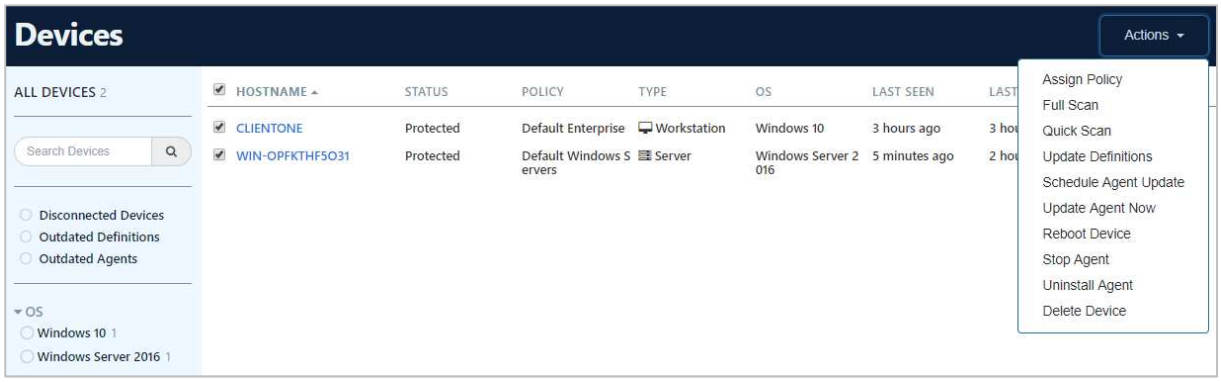
This can be seen by opening the *Devices* page and clicking on an individual client to see its properties:



Managing the network

Scanning, scheduling scans, updates and removing devices from the console

These tasks can all be carried out from the *Devices* page, by selecting clients' check boxes, then clicking the *Action* menu:

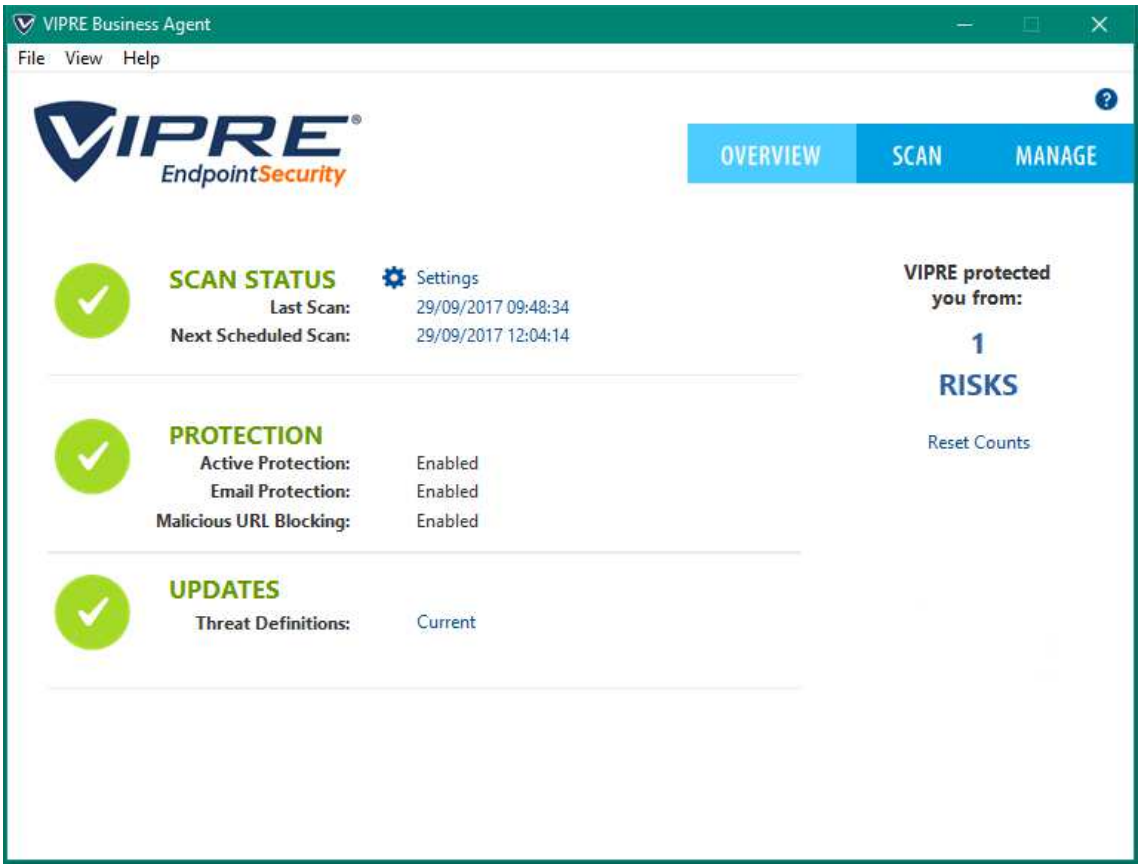


Controlling user access to the endpoint protection software

By default, users cannot disable protection features on the endpoint protection software.

Windows client endpoint protection software

There is a full GUI, similar to a consumer antivirus program:



Tasks available to users

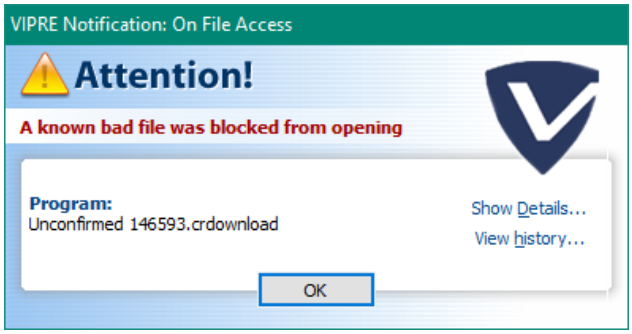
Users can see status, and run scans and updates.

Windows Security Center/Windows Defender

VIPRE Business Agent registers in Windows Security Center as the antivirus program. Windows Defender is disabled.

Alerts

If the EICAR test file is downloaded, the alert below is shown:



No user action is required. The alert persists until closed by the user.

If real-time protection is disabled, the status display in the main program window changes to show a warning:

Protection can only be reactivated from the console.

Windows Server endpoint protection software

This can be regarded as identical to the client software.

Features (as of September 2017)	Avast Business Antivirus	Barracuda NextGen Firewall	Bitdefender GravityZone Cloud	Crowdstrike Falcon Endpoint Protection	Emsisoft Enterprise Console	Endgame Protection Platform	ESET Remote Administrator	F-Secure Protection Service for Business	FortiClient Enterprise Management Server	G DATA Business Security	Kaspersky Endpoint Security for Business Advanced	Panda Adaptive Defense 360	Palo Alto Networks Traps	SentinelOne Endpoint Protection	Trend Micro OfficeScan XG	VIPRE Cloud
Console type and features																
Console type																
Cloud-based console	●		●	●		●		●		●		●		●	●	●
On-premise Windows-based console	●	●			●	●	●		●	●	●		●		●	
On-premise virtual appliance	●	●	●			●	●			●			●	●	●	
Minimum hardware requirements for Windows-based console																
CPU (GHz), RAM (GB)	2 GHz, 4 GB	1 GHz, 4 GB	N/A	N/A	2 GHz, 1 GB	2 GHz, 1 GB	2x2 GHz, 4 GB	N/A	2x2 GHz, 4 GB	2 GHz, 1 GB	1 GHz, 4GB	N/A	2.2 GHz, 4 GB	N/A	2 GHz, 2 GB	N/A
Supported virtualisation systems for virtual appliances																
VMware vSphere		●	●	●		●	●			●		●		●		
VMware ESXi		●	●	●		●	●			●	●	●		●	●	
VMware Workstation			●	●		●	●			●		●	●	●	●	
VMware Player			●	●		●	●			●		●	●			
Oracle Virtual Box			●	●		●	●			●		●	●	●		
Microsoft Hyper-V		●	●	●		●	●			●	●	●	●	●	●	
Citrix Xen Server		●	●	●		●	●			●	●	●	●		●	
Citrix Xen Desktop	●		●	●		●	●			●	●	●	●		●	
Client software deployment methods																
Push installation from the console	●	●	●		●	●	●		●	●	●	●			●	
Email a link to remote users to install the software themselves	●		●	●		●		●	●	●		●		●	●	●
Creation of .exe or .msi installer package	●	●	●	●	●	●	●	●	●	●	●	●		●	●	●
Client management actions that can be run from the console																
Update product modules / detection engine / definitions	●	●	●	●	●	●	●			●	●	●	●	●	●	●
Reboot computer	●		●			●	●				●			●		●
Scan computer	●		●		●	●	●	●	●	●	●	●		●	●	●
Enable/Disable On-Access Scan and/or Firewall	●		●		●	●	●	●	●	●	●	●		●	●	●
Supported Server OS																
Microsoft Windows servers	Management Console / Protection client	Management Console / Protection client	Management Console / Protection client	Management Console / Protection client	Management Console / Protection client	Management Console / Protection client	Management Console / Protection client	Management Console / Protection client	Management Console / Protection client	Management Console / Protection client	Management Console / Protection client	Management Console / Protection client	Management Console / Protection client	Management Console / Protection client	Management Console / Protection client	Management Console / Protection client
Windows Server 2008 32-bit	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Windows Server 2008 64-bit/2008 R2/2012/R2/2016 64-bit Std/Essentials	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Windows Small Business Server 2008/2011 64-bit	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Supported Desktop OS																
Microsoft Windows clients	Management Console / Protection client	Management Console / Protection client	Management Console / Protection client	Management Console / Protection client	Management Console / Protection client	Management Console / Protection client	Management Console / Protection client	Management Console / Protection client	Management Console / Protection client	Management Console / Protection client	Management Console / Protection client	Management Console / Protection client	Management Console / Protection client	Management Console / Protection client	Management Console / Protection client	Management Console / Protection client
Windows XP SP3																
Home/Professional/Media Center Edition 32-bit / 64-bit	●	●	N/A	N/A	●	N/A	●	●	N/A		●	●	●	●	●	N/A
Windows 7 / 8 / 8.1 / 10																
Home Premium/Consumer 32-bit / 64-bit	●	●	N/A	N/A	●	N/A	●	●	N/A	●	●	●	●	●	●	●
Pro/Ultimate/Education/Enterprise 32-bit / 64-bit	●	●	N/A	N/A	●	N/A	●	●	N/A	●	●	●	●	●	●	●
Apple Mac OS clients	Management Console / Protection client	Management Console / Protection client	Management Console / Protection client	Management Console / Protection client	Management Console / Protection client	Management Console / Protection client	Management Console / Protection client	Management Console / Protection client	Management Console / Protection client	Management Console / Protection client	Management Console / Protection client	Management Console / Protection client	Management Console / Protection client	Management Console / Protection client	Management Console / Protection client	Management Console / Protection client
OS X 10.7 and higher	●	●	N/A	N/A	●	N/A	●	●	N/A	●	●	●	●	●	●	N/A
Supported Mobile OS																
Google Android clients																
4.4 and higher							●	●		●	●				●	
Apple iOS clients																
9.0 and higher							●	●		●	●				●	
Client-Software Features																
Microsoft Windows clients																
Antimalware	●		●	●	●	●	●	●	●	●	●	●	●	●	●	●
Antispam	●		●				●	●		●		●	●		●	●
Data backup							●			●				●		
Data or Email encryption			●				●				●				●	
Device control			●				●			●	●	●		●	●	
Firewall	●		●				●	●		●	●	●			●	●
Phishing protection	●		●		●		●	●	●	●	●	●	●		●	●
Settings & Uninstall protection	●		●	●	●	●	●	●	●	●	●	●	●	●	●	●
EDR (Endpoint Detection and Response)			available in separate product (Bitdefender xDR - Q4/2017)	●		●	available in separate product (ESET Enterprise Inspector)		available in separate product (Fortinet FortiAnalyzer)		available in next version (KES 11 - Q4/2017)	●		●	available in separate product (Trend Micro Endpoint Sensor)	
Web access control			●		●		●	●	●	●	●	●			●	●
Apple Mac OS clients																
Antimalware	●		●	●			●	●	●	●	●	●	●	●	●	
Device control							●								●	
Firewall							●									
Phishing protection	●		●				●	●	●	●	●		●			
Settings & Uninstall protection	●		●				●		●	●	●	●	●	●	●	
Web access control							●	●	●						●	
Google Android clients																
Antimalware							●	●		●	●	●	●		●	
App control							●			●	●				●	
Call/text-message blocker							●			●	●				●	
Phishing protection							●			●	●		●			
Settings & Uninstall protection							●			●	●				●	
Theft protection							●	●		●	●	●			●	
General																
Support																
Telephone & Email support	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Remote control by support staff available	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Support forum	●	●	●	●	●	●	●	●	●		●	●	●	●	●	●
Chat support	●	●	●	●		●	●	●	●	●	●	●		●	●	●
Languages:																
Which languages can be used to contact support?	English, Spanish, French, German, Italian, Portuguese, Russian, Norwegian	English, German, French, Italian, Spanish	English, Spanish, German, Romanian, French	English	English, German, French, Russian, Italian	English	All	English, Japanese, Finnish, Swedish, German, French, Danish, Norwegian	English, French, German, Japanese, Chinese	German, English, Italian, Spanish, French	English, Russian, German, French, Spanish, Italian, Portuguese, Japanese, Polish, Dutch, Danish, Finnish, Norwegian, Swedish, Turkish, Arabic, Chinese, Korean, Hindi, Malay	English, Spanish, Italian, French, Swedish, German, Polish, Dutch, Portuguese, Russian	English, French, German, Italian, Japanese, Korean, Portuguese, Chinese, Spanish	English, Chinese, Hebrew, French, German	English	English
Which interface languages is the product available in?	English, Spanish, French, German, Italian, Portuguese, Russian, Norwegian	English	English, Spanish, German, Romanian, French, Italian, Portuguese, Polish, Russian		English, German, French, Russian, Italian, Spanish, Arabic, Catalan, Persian, Finnish, Greek, Hungarian, Japanese, Korean, Dutch, Polish, Portuguese, Slovenian, Swedish, Thai, Turkish, Vietnamese, Chinese		English, German, Spanish, Spanish Latin, French Canadian, Greek, Turkish, French, Russian, Polish, Italian, Japanese, Chinese, Arabic, Slovak, Czech, Croatian, Korean	English, Chinese, Czech, Danish, Dutch, Estonian, Finnish, French, German, Greek, Hungarian, Italian, Japanese, Korean, Norwegian, Polish, Portuguese, Romanian, Russian, Slovenian, Spanish, Swedish, Turkish	English, Chinese, French, German, Japanese, Korean, Portuguese, Spanish	German, English, Italian, Spanish, French, Polish, Portuguese, Chinese	English, Arabic, Polish, Korean, Italian, German, French,Chinese, Turkish, Spanish, Russian, Romanian, Portuguese, Dutch, Polish, Hungarian, Vietnamese, Czech	English, Spanish, French, Italian, Portuguese, Swedish, German, Hungarian, Russian	English, French, Spanish, Chinese, Japanese, German		English, German, Spanish, French, Italian, Japanese, Korean, Polish, Russian, Chinese	
Which languages are the manuals available in?					English				English	German, English, French, Spanish, Polish, Chinese		English, Spanish				
Pricing (approximate prices as of September 2017)																
25 clients																
1 year $ US	800	700	900	N/A	450	N/A	785	845	175	800	1.425	1.700	N/A	N/A	950	750
3 years $ US	1.440	2.100	1.790		1.080		1.570	2.110	525	1.600	2.849	4.075			2.100	2.250
1 year € DE	670	700	765		450		665	845	175	800	1.430	1.700			950	650
3 years € DE	1.210	2.100	1.530		1.080		1.330	2.110	525	1.600	3.220	4.075			2.100	1.950
500 clients																
1 year $ US	8.995	3.500	11.200	32.065	5.975	12.500	10.210	7.855	5.300	10.000	17.520	22.000	20.000	32.500	16.875	9.500
3 years $ US	16.190	10.500	22.400	86.575	14.375	37.500	20.425	19.635	15.900	20.000	35.035	52.800	48.000	73.000	50.625	28.500
1 year € DE	7.555	3.500	8410	27.255	5.975	12.500	8.650	7.855	4.750	10.000	16.705	22.000	19.595	32.500	16.875	8000
3 years € DE	13.600	10.500	16.820	73.590	14.375	37.500	17.300	19.635	12.500	20.000	37.585	52.800	47.035	73.000	50.635	24.000
1000 clients																
1 year $ US	17.970	5.000	21.350	51.955	9.950	25.000	18.655	15.710	10.600	17.500	31.570	37.000	37.000	55.000	33.750	19.000
3 years $ US	32.350	15.000	42.700	140.260	23.950	75.000	37.305	39.270	31.800	35.000	63.140	88.000	81.600	124.000	101.250	57.000
1 year € DE	15.095	5.000	15980	44.160	9.950	25.000	15.800	15.710	9.500	17.500	30.000	37.000	36.655	55.000	33.750	16.000
3 years € DE	27.175	15.000	31.960	119.220	23.950	75.000	31.600	39.270	25.000	35.000	67.510	88.000	79.960	124.000	101.250	48.000
Minimum number of seats to get the product																
Seats	1	5	5	130	1	250	5	1	1	5	5	1	200	100	1	5

Copyright and Disclaimer

This publication is Copyright © 2017 by AV-Comparatives®. Any use of the results, etc. in whole or in part, is ONLY permitted after the explicit written agreement of the management board of AV-Comparatives, prior to any publication. AV-Comparatives and its testers cannot be held liable for any damage or loss, which might occur as result of, or in connection with, the use of the information provided in this paper. We take every possible care to ensure the correctness of the basic data, but a liability for the correctness of the test results cannot be taken by any representative of AV-Comparatives. We do not give any guarantee of the correctness, completeness, or suitability for a specific purpose of any of the information/content provided at any given time. No one else involved in creating, producing or delivering test results shall be liable for any indirect, special or consequential damage, or loss of profits, arising out of, or related to, the use or inability to use, the services provided by the website, test documents or any related data.

For more information about AV-Comparatives and the testing methodologies, please visit our website.

(October 2017)